

Nessus 5.2-Installations- und Konfigurationshandbuch

9. Januar 2014

(Revision 18)



Inhaltsverzeichnis

Einleitung

Das vorliegende Dokument beschreibt die Installation und Konfiguration des Sicherheitslückenscanners **Nessus 5.2** von Tenable Network Security. Wir freuen uns über Ihre Anmerkungen und Vorschläge. Senden Sie diese an support@tenable.com.

Tenable Network Security, Inc. hat den Nessus Sicherheitslückenscanner entwickelt und pflegt diese Software. Tenable arbeitet nicht nur fortlaufend an der Optimierung der Nessus-Engine, sondern entwickelt auch die meisten für diesen Scanner erhältlichen Plugins sowie Compliancetests und eine Vielzahl von Auditrichtlinien.

Im vorliegenden Dokument werden Voraussetzungen und Bereitstellungsoptionen beschrieben. Außerdem finden Sie hier eine Schrittanleitung der Installation. Grundlegende Kenntnisse zu UNIX und zu Sicherheitslückenscannern werden dabei vorausgesetzt.

Regeln und Konventionen

In der gesamten Dokumentation werden Dateinamen, Daemons und ausführbare Dateien in einer Schriftart wie **courier bold** angezeigt (Beispiel: **setup.exe**).

Befehlszeilenoptionen und Schlüsselwörter werden ebenfalls in der Schriftart **courier bold** angezeigt. Die Befehlszeilen sind teils mit, teils ohne Befehlszeilen-Prompt und den Ausgabetext des betreffenden Befehls aufgeführt. In den Befehlszeilen erscheint der ausgeführte Befehl in der Schriftart **courier bold**, um zu verdeutlichen, was der Benutzer eingegeben hat. Die vom System generierte Beispielausgabe ist hingegen in der Schriftart courier (ohne Fettdruck) aufgeführt. Es folgt ein Beispiel für die Ausführung des UNIX-Befehls **pwd**:

```
# pwd
/opt/nessus/
#
```



Wichtige Hinweise und Aspekte werden durch dieses Symbol und graue Textfelder hervorgehoben.



Tipps, Beispiele und Best Practices (Empfehlungen) werden durch dieses Symbol und weißen Text auf blauem Grund hervorgehoben.

Organisation

Da unabhängig vom verwendeten Betriebssystem die Nessus-Benutzeroberfläche verwendet wird, sind in diesem Dokument zunächst die systemspezifischen Informationen aufgeführt. Die betriebssystemübergreifenden Funktionalitäten werden nachfolgend beschrieben.

Neue Funktionen in Nessus 5.2



Beginnend mit Nessus 5 erfolgt die Konfiguration von Benutzerverwaltung und Nessus-Server (Daemon) nicht mehr über den eigenständigen NessusClient oder die Datei **nessusd.conf**, sondern über die Nessus-Benutzeroberfläche. Die Nessus-Benutzeroberfläche ist eine webbasierte Oberfläche für Konfiguration, Richtlinienerstellung, Scans und die gesamte Berichterstellung.

Seit dem 22. August 2013 haben die Nessus-Produkte folgende neue Namen:

Ehemaliger Produktname	Neuer Produktname
Nessus ProfessionalFeed	Nessus
Nessus HomeFeed	Nessus Home

Folgende Aufstellung zeigt die offiziellen Nessus-Produktnamen:

- Nessus®
- Nessus Perimeter Service
- Nessus Auditor Bundles
- Nessus Home

Änderungen bei den wichtigsten Funktionen

Nachfolgend aufgeführt sind einige neue Funktionen in Nessus 5.2. Eine vollständige Liste der Änderungen finden Sie in den Versionshinweisen im Diskussionsforum.

- IPv6 wird jetzt bei den meisten Windows-Installationen unterstützt.
- Der Aktivierungscode zur Registrierung wird Ihnen in Nessus während der Installation bereitgestellt.
- Nessus kann optional während des Sicherheitslückenscans Screenshots erstellen, die dem Bericht als Nachweis der Sicherheitslücke hinzugefügt werden.
- Unter Mac OS X gibt es nun einen Bereich für Systemvoreinstellungen zur Nessus-Serviceverwaltung.
- Digital signierte Nessus-RPM-Pakete für unterstützte Distributionen
- Geringerer Bedarf an Arbeits- und Festplattenspeicher
- Schnellere, benutzerfreundliche Weboberfläche mit geringerem Bandbreitenbedarf
- Neue NASL-Funktionen für komplexere, aber codesparende Plugins
- Nach Abschluss des Scans werden die Ergebnisse automatisch an den Benutzer gesendet.

Unterstützte Betriebssysteme

Nessus wird für eine Vielzahl von Betriebssystemen und Plattformen angeboten und unterstützt:

- Debian 6 (i386 und x86-64)
- Fedora Core 16, 17 und 18 (i386 und x86-64)
- FreeBSD 9 (i386 und x86-64)
- Mac OS X 10.8 und 10.9 (i386 und x86-64)
- Red Hat ES 4/CentOS 4 (i386)
- Red Hat ES 5/CentOS 5/Oracle Linux 5 (i386 und x86-64)
- Red Hat ES 6/CentOS 6/Oracle Linux 6 (i386 und x86-64) [Server, Desktop, Workstation]
- SuSE 10 (x86-64) und 11 (i386 und x86-64)
- Ubuntu 10.04 (9.10 Paket), 11.10, 12.04 und 12.10 (i386 und x86-64)
- Windows XP, Server 2003, Server 2008, Server 2008 R2*, Server 2012, Vista, 7 und 8 (i386 und x86-64)



Beachten Sie, dass die Version von Microsoft Internet Explorer, die Bestandteil von Windows Server 2008 R2 ist, Java-Installationen nicht einwandfrei unterstützt. Dies führt dazu, dass Nessus in bestimmten Situationen nicht erwartungsgemäß funktioniert. Des Weiteren rät die Microsoft-Richtlinie von der Verwendung von Internet Explorer unter Serverbetriebssystemen ab.



Nessus verwendet verschiedene Drittanbieter-Softwarepakete, die unter unterschiedlicher Lizenz verteilt werden. Wenn Sie `nessusd` (bzw. unter Windows `nessusd.exe`) mit dem Argument `–l` ausführen, wird eine Liste dieser Softwarelizenzen von Drittanbietern angezeigt.

Hintergrund

Nessus ist ein leistungsfähiger und benutzerfreundlicher Sicherheitsscanner für Ihr Netzwerk. Er umfasst eine umfangreiche Plugin-Datenbank, die täglich aktualisiert wird. Er zählt gegenwärtig in der gesamten Security-Branche zu den besten Produkten seiner Art und wird durch professionelle Datensicherheitsorganisationen wie das SANS Institute beworben und gefördert. Nessus ermöglicht es Ihnen, eine Fernüberwachung Ihres Netzwerks durchzuführen und festzustellen, ob Unbefugte in das Netzwerk eingedrungen sind oder ein Missbrauch der Netzwerkfunktionen aufgetreten ist. Nessus bietet zudem die Möglichkeit, ein bestimmtes System lokal auf Sicherheitslücken, die Erfüllung von Compliancespezifikationen, eine Verletzung der Inhaltsrichtlinien usw. zu prüfen.

- **Intelligentes Scannen**. Anders als bei vielen anderen Sicherheitsscannern wird von Nessus nichts als gegeben vorausgesetzt. Es wird nicht erwartet, dass ein gegebener Dienst über einen bestimmten Port ausgeführt wird. Wenn Sie also Ihren Webserver über den Port 1234 betreiben, wird dies von Nessus erkannt, und die Sicherheitstests werden entsprechend ausgeführt. Wann immer es möglich ist, wird versucht, eine Sicherheitslücke durch die tatsächliche Nutzung zu bewerten. In anderen Fällen, in denen eine solche Vorgehensweise nicht zuverlässig ist oder negative Auswirkungen auf das Ziel haben kann, nutzt Nessus unter Umständen ein Serverbanner, um das Vorhandensein einer Sicherheitslücke zu ermitteln. In diesem Fall geht aus dem Ausgabebericht eindeutig hervor, ob diese Methode verwendet wurde.

- **Modulare Architektur**. Die Client/Server-Architektur bietet die erforderliche Flexibilität, um den Scanner (Server) bereitzustellen und eine Verbindung mit dem GUI (grafische Benutzeroberfläche, Client) herzustellen, der auf einem beliebigen Computer in einem Webbrowser ausgeführt wird. Diese Vorgehensweise senkt die Verwaltungskosten, da mehrere Clients auf denselben Server zugreifen können.

- **CVE-Kompatibilität**. Die meisten Plugins verweisen auf die CVE, damit Administratoren weitere Informationen zu veröffentlichten Sicherheitslücken abrufen können. Häufig sind auch Referenzen in BugTraq (BID), OSVDB und bei anderen Anbietern von Sicherheitswarnungen angegeben.

- **Plugin-Architektur**. Alle Sicherheitstests werden als externes Plugin entwickelt und dann einer von 42 Plugin-Familien zugeordnet. Auf diese Weise können Sie ganz einfach eigene Tests hinzufügen, bestimmte Plugins auswählen oder eine ganze Familie nutzen, ohne den Code der Nessus-Server-Engine `nessusd` lesen zu müssen. Eine vollständige Liste der Nessus-Plugins finden Sie unter http://www.nessus.org/plugins/index.php?view=all.

- **NASL**. Der Nessus-Scanner umfasst die NASL-Sprache (Nessus Attack Scripting Language). NASL wurde speziell zur schnellen und einfachen Entwicklung von Sicherheitstests entworfen.

- **Aktuelle Sicherheitslücken-Datenbank**. Tenable legt bei der Entwicklung von Sicherheitstests den Schwerpunkt auf neu entdeckte Sicherheitslücken. Die Datenbank mit den Sicherheitstests wird täglich aktualisiert. Die aktuellsten Sicherheitstests stehen unter http://www.tenable.com/plugins/index.php?view=newest zum Download bereit.

- **Gleichzeitiger Test mehrerer Hosts**. Abhängig von der Konfiguration Ihres Nessus-Scannersystems können Sie eine große Zahl Hosts gleichzeitig testen.

- **Intelligente Diensterkennung**. Nessus setzt nicht voraus, dass sich die Zielhosts nach den von der IANA zugewiesenen Portnummern richten. Ein FTP-Server, der über einen anderen als den Standardport ausgeführt wird (z. B. Port 31337), wird ebenso erkannt wie ein Webserver, der Port 8080 statt Port 80 nutzt.

- **Mehrere Dienste**. Wenn zwei oder mehr Webserver auf einem Host ausgeführt werden (z. B. einer auf Port 80 und ein zweiter auf Port 8080), dann werden sie alle von Nessus erkannt und getestet.

- **Plugin-Kooperation**. Die von Nessus-Plugins ausgeführten Tests kooperieren, d. h. es werden keine unnötigen Tests ausgeführt. Wenn Ihr FTP-Server keine anonymen Anmeldungen bietet, dann werden für anonyme Anmeldungen relevante Sicherheitstests nicht ausgeführt.

- **Umfassende Berichterstattung**. Mit Nessus erfahren Sie nicht nur, welche Sicherheitslücken in Ihrem Netzwerk vorhanden sind und welches Risikoausmaß sie jeweils darstellen (Hinweis, niedrig, moderat, hoch oder kritisch), sondern erhalten auch Informationen zu Lösungen, um diese Lücken zu schließen.

- **Vollständige SSL-Unterstützung**. Nessus kann auch Dienste testen, die über SSL vermittelt werden (z. B. HTTPS, SMTPS, IMAPS usw.).

- **Smart-Plugins (optional)**. Nessus bietet eine Optimierungsoption, die selbsttätig feststellt, mit welchen Plugins ein Remotehost getestet werden soll – und mit welchen nicht. Beispielsweise werden sendmail-Sicherheitslücken von Nessus nicht für Postfix ausgeführt.

- **Nichtdestruktiver Betrieb (optional)**. Einige Tests wirken sich negativ auf bestimmte Netzwerkdienste aus. Wenn Sie das Risiko eines Dienstausfalls in Ihrem Netzwerk nicht eingehen möchten, aktivieren Sie die Nessus-Option „Safe Checks" („Sichere Tests"). In diesem Fall nutzt Nessus Banner zur Überprüfung darauf, ob eine Sicherheitslücke vorhanden ist, statt Fehler tatsächlich zu nutzen.

- **Offenes Forum**. Sie haben einen Bug gefunden? Oder eine Frage zu Nessus? Beteiligen Sie sich am Forum unter https://discussions.nessus.org/.

Voraussetzungen

Tenable empfiehlt je nach Einsatzweise von Nessus die folgende Hardware. Beachten Sie, dass diese Ressourcen speziell für den Einsatz von Nessus empfohlen werden. Bei Ausführen weiterer Software oder einer zusätzlichen Systembelastung sind weitere Ressourcen erforderlich.

Szenario	CPU/Arbeitsspeicher	Festplattenspeicher
Nessus-Scan kleinerer Netzwerke	CPU: 1 × Pentium 4 DualCore, 2 GHz (Intel® DualCore für Mac OS X) Arbeitsspeicher: 2 GB RAM (4 GB RAM empfohlen)	30 GB
Nessus-Scans größerer Netzwerke einschließlich Audit-Trails und Erstellung von PDF-Berichten	CPU: 1 × Pentium 4 DualCore, 3 GHz (2 DualCore-CPUs empfohlen) Arbeitsspeicher: 3-4 GB RAM (8 GB RAM empfohlen)	30 GB

Nessus kann in einer VMware-Instanz ausgeführt werden. Wenn die virtuelle Maschine jedoch die Netzadress-übersetzung (Network Address Translation, NAT) für die Verbindung mit dem Netzwerk verwendet, kann dies zahlreiche Sicherheitstests, die Hostauflistung und die Betriebssystemerkennung von Nessus beeinträchtigen.

Nessus UNIX

Für die Installation von Nessus unter UNIX/Linux müssen verschiedene Bibliotheken vorhanden sein. Viele Betriebs-systeme installieren diese standardmäßig, weswegen eine separate Installation in der Regel nicht erforderlich ist:

- zlib
- GNU C-Bibliothek (d. h. libc)
- Oracle Java (nur für die PDF-Berichterstellung)



Java muss vor der Nessus-Installation auf dem Host installiert werden. Wird Java nach der Nessus-Installation installiert, muss Nessus neu installiert werden.

Nessus Windows

Microsoft hat an Windows XP SP2 und nachfolgenden Windows-Versionen Änderungen vorgenommen, die die Leistungsfähigkeit von Nessus Windows beeinträchtigen können. Um die Leistungsfähigkeit und die Zuverlässigkeit von Scans zu steigern, wird dringend empfohlen, Nessus Windows auf einem Serverprodukt der Microsoft Windows-Familie

(z. B. Windows Server 2003) zu installieren. Weitere Informationen zu diesem Thema finden Sie unter „Problembehandlung bei Nessus für Windows“.

Bereitstellungsoptionen

Für die Bereitstellung von Nessus sind Kenntnisse in den Bereichen Routing, Filter und Firewallrichtlinien häufig sehr nützlich. Wir empfehlen, Nessus so bereitzustellen, dass eine ausreichende IP-Konnektivität zu den zu scannenden Netzwerken besteht. Die Bereitstellung hinter einem NAT-Gerät wird nur für Scans im internen Netzwerk empfohlen. Wenn ein Sicherheitslückenscan einen NAT- oder Anwendungsproxy passieren muss, kann der Test verfälscht werden. In solchen Fällen kann es zu Fehlalarmen, aber auch zum Übersehen von Sicherheitslücken kommen. Außerdem können Personal Firewalls oder Desktop-Firewalls, die auf demselben System vorhanden sind, auf dem Nessus ausgeführt wird, die Wirksamkeit eines remote ausgeführten Sicherheitslückenscans erheblich beeinträchtigen.



Hostbasierte Firewalls können Sicherheitslückenscans im Netzwerk stören. Abhängig von der Konfiguration Ihrer Firewall können die Probes (Testdaten) eines Nessus-Scans verworfen, beschädigt oder verborgen werden.



Bestimmte Netzwerkgeräte, die eine zustandsbezogene Inspektion ausführen (z. B. Firewalls, Lastausgleichs-module oder Intrusion-Detection- bzw. Intrusion-Prevention-Systeme), können negativ reagieren, wenn sie bei einem Scan überprüft werden. Nessus bietet eine Reihe von Optimierungsoptionen, mit denen sich die Auswirkungen des Scannens solcher Geräte einschränken lassen. Allerdings lassen sich Probleme in Verbindung mit dem Scannen solcher Netzwerkgeräte am besten vermeiden, indem Sie einen authentifizierten Scan durchführen.

Hostbasierte Firewalls

Wenn Ihr Nessus-Server auf einem Host mit einer Personal Firewall wie beispielsweise ZoneAlarm, der Windows-Firewall oder einer anderen Firewallsoftware konfiguriert ist, müssen Verbindungsanfragen von der IP-Adresse des Nessus-Clients zugelassen werden.

Standardmäßig wird für den Nessus-Webserver (d. h. die Benutzeroberfläche) Port 8834 verwendet. Auf Systemen unter Microsoft XP Service Pack 2 (SP2) und höher erhält der Benutzer nach einem Klick auf das „**Sicherheitscenter**“ in der „**Systemsteuerung**“ die Möglichkeit, die Einstellungen der Windows-Firewall zu verwalten. Um Port 8834 zu öffnen, wählen Sie die Registerkarte „**Ausnahmen**“ aus und fügen Sie Port 8834 zur Liste hinzu.

Bei anderen Personal Firewalls ziehen Sie die Dokumentation des Anbieters zurate, um diese Konfiguration durchzuführen.

Sicherheitslücken-Plugins

Tag für Tag werden zahlreiche neue Sicherheitslücken von Anbietern, Wissenschaftlern und anderen Quellen publik gemacht. Ziel von Tenable ist es, Tests für neu veröffentlichte Sicherheitslücken möglichst schnell zu testen und verfügbar zu machen. Im Normalfall geschieht dies innerhalb von 24 Stunden nach der Veröffentlichung. Ein Testmodul für eine bestimmte Sicherheitslücke heißt in der Terminologie des Nessus-Scanners „Plugin“. Eine vollständige Liste der Nessus-Plugins finden Sie unter http://www.tenable.com/plugins/index.php?view=all. Tenable verteilt Plugins für die aktuellsten Sicherheitslücken in zwei verschiedenen Modi: Nessus und Nessus Home.

Plugins werden direkt von Tenable heruntergeladen. Dies geschieht über einen automatisierten Prozess in Nessus. Nach dem Download überprüft Nessus die digitalen Signaturen aller heruntergeladenen Plugins, um die Dateiintegrität sicherzustellen. Für Nessus-Installationen ohne Internetzugang gibt es einen Offlineupdateprozess, mit dem sich sicherstellen lässt, dass der Scanner auf dem aktuellen Stand bleibt.



Sie müssen sich für Plugins registrieren und diese aktualisieren, bevor Sie Nessus starten und die Scanoberfläche von Nessus angezeigt wird. Das Plugin-Update läuft nach der Erstregistrierung des Scanners im Hintergrund ab und kann mehrere Minuten dauern.

Nessus Produkttypen

Tenable bietet über das Tenable Support Portal oder via E-Mail kostenpflichtigen Support für Nessus-Kunden, die Version 5 oder höher einsetzen. Ebenfalls in Nessus enthalten ist eine Anzahl hostbasierter Compliancetests für UNIX und Windows. Diese sind sehr nützlich bei der Ausführung von Compliance-Audits nach den Vorgaben von SOX, FISMA oder PCI DSS.

Sie können Nessus entweder über den Onlinestore von Tenable unter https://store.tenable.com/ oder bei einem autorisierten Nessus-Partner erwerben. Danach erhalten Sie von Tenable einen Aktivierungscode. Diesen Code verwenden Sie bei der Updatekonfiguration Ihrer Nessus-Kopie.



Wenn Sie Nessus in Verbindung mit Tenable SecurityCenter verwenden, aktualisiert SecurityCenter Ihre Nessus-Scanner automatisch.

Wohltätigkeitsorganisationen im Sinne des Abschnitts 501(c)(3) des US-amerikanischen Internal Revenue Code haben unter Umständen Anspruch auf eine kostenfreie Nutzung von Nessus. Weitere Informationen finden Sie auf der Webseite „Tenable Charitable Organization Subscription Program" („Tenable-Abonnementprogramm für Wohltätigkeits-organisationen").

Für Benutzer, die Nessus zu Hause und nichtkommerziell einsetzen, ist Nessus Home gedacht. Die Nutzung von Nessus Home ist kostenfrei. Allerdings gibt es für Nessus Home eine separate Lizenz, die der Benutzer akzeptieren muss.

IPv6-Unterstützung

Nessus unterstützt das Scannen IPv6-basierter Ressourcen. Viele Betriebssysteme und Geräte bieten mittlerweile standardmäßig aktivierte IPv6-Unterstützung. Um Scans von IPv6-Ressourcen durchzuführen, muss mindestens eine IPv6-Schnittstelle auf dem Host konfiguriert sein, auf dem Nessus installiert ist. Zudem muss sich Nessus in einem IPv6-fähigen Netzwerk befinden (Nessus kann IPv6-Ressourcen über IPv4 nicht scannen, aber IPv6-Schnittstellen über authentifizierte Scans über IPv4 auflisten). Bei Scans werden sowohl die vollständige als auch die verkürzte IPv6-Notation unterstützt.



In älteren Versionen von Microsoft Windows fehlen einige wichtige APIs, die für den Nachbau von IPv6-Paketen erforderlich sind (z. B. zum Abruf der MAC-Adresse des Routers, der Routingtabelle usw.). Hierdurch wird ein ordnungsgemäßes Funktionieren des Portscanners verhindert. Aus diesem Grund ist eine IPv6-Unterstützung unter Windows XP und Server 2003 nicht gegeben.



Das Scannen von IPv6 Global Unicast-IP-Adressbereichen wird nur unterstützt, wenn die IP-Adressen separat (d. h. im Listenformat) eingegeben werden. Nessus unterstützt keine Bereichsangaben, die mit Bindestrichen getrennt oder als CIDR-Adressen angegeben sind. Link-Local-Adressbereiche werden hingegen bei Verwendung der Direktive „link6" Anweisung als Scanziel oder als Local-Link mit „%eth0" unterstützt.

Upgrade von einer Test- auf eine Lizenzversion

Wenn Sie Nessus im Rahmen einer Testlizenz installiert haben, wird dringend empfohlen, diese Version zu deinstallieren, bevor Sie zur lizensierten Vollversion wechseln. Alle von Ihnen erstellten Richtlinien oder Scanergebnisse können exportiert und dann in die neue Installation importiert werden.

UNIX/Linux

Upgrade ausführen

In diesem Abschnitt wird erläutert, wie ein Upgrade einer vorhandenen Nessus-Installation ausgeführt wird.

Laden Sie die aktuelle Nessus-Version von http://www.tenable.com/products/nessus/select-your-operating-system oder über das Tenable Support Portal herunter. Überprüfen Sie die Integrität des Installationspakets. Hierzu vergleichen Sie die MD5-Prüfsumme der heruntergeladenen Datei mit der in der Datei **`MD5.asc`** (hier) angegebenen Prüfsumme.



Sofern nicht anders angegeben, müssen alle Befehle als Benutzer `root` des Systems ausgeführt werden. Normale Benutzerkonten verfügen gewöhnlich nicht über die zur Installation dieser Software erforderlichen Berechtigungen.

In der folgenden Tabelle finden Sie Hinweise zu Upgrades für den Nessus-Server auf allen in der Vergangenheit unterstützten Plattformen. Zuvor erstellte Konfigurationseinstellungen und Benutzer werden unverändert übernommen.



Stellen Sie sicher, dass eine laufende Ausführung von Scans abgeschlossen wurde, bevor Sie **`nessusd`** anhalten.

Spezielle Upgradehinweise finden Sie jeweils in einer auf das Beispiel folgenden Anmerkung.

Plattform	**Upgradeanleitung**
Red Hat ES 4 und CentOS 4 (32-Bit); Red Hat ES 5, CentOS 5 und Oracle Linux 5 (32- und 64-Bit); Red Hat ES 6, CentOS 6 und Oracle Linux 6 (32- und 64-Bit)	

Upgradebefehle	`# service nessusd stop`
	
	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Red Hat-Version:
	
	`# rpm -Uvh Nessus-5.2.4-es4.i386.rpm`
	`# rpm -Uvh Nessus-5.2.4-es5.i386.rpm`
	`# rpm -Uvh Nessus-5.2.4-es5.x86_64.rpm`
	`# rpm -Uvh Nessus-5.2.4-es6.i686.rpm`
	`# rpm -Uvh Nessus-5.2.4-es6.x86_64.rpm`
	
	Nach Abschluss des Upgrades starten Sie den Dienst **`nessusd`** mit dem folgenden Befehl neu:
	
	`# service nessusd start`

Beispielausgabe	`# service nessusd stop`
	`Shutting down Nessus services:                    [ OK ]`
	`# rpm -Uvh Nessus-5.2.4-es5.i386.rpm`
	`Preparing... ########################################### [100%]`
	`Shutting down Nessus services: /etc/init.d/nessusd: … 1:Nessus`
	`########################################### [100%]`
	`Fetching the newest plugins from nessus.org...`
	`Fetching the newest updates from nessus.org...`
	`Done. The Nessus server will start processing these plugins within a minute`
	`nessusd (Nessus) 5.2.4 [build R23016] for Linux`
	`(C) 1998 - 2013 Tenable Network Security, Inc.`
	
	`Processing the Nessus plugins...`
	`[##################################################]`
	
	`All plugins loaded`
	` - You can start nessusd by typing /sbin/service nessusd start`
	` - Then go to https://localhost:8834/ to configure your scanner`
	`# service nessusd start`
	`Starting Nessus services:                    [ OK ]`

<table>
<tr><td></td><td>#</td></tr>
<tr><th colspan="2">Fedora Core 16, 17 und 18 (32- und 64-Bit)</th></tr>
<tr><td>Upgradebefehle</td><td><code># service nessusd stop</code>

Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Fedora Core-Version:

<code># rpm -Uvh Nessus-5.2.4-fc16.i686.rpm</code>
<code># rpm -Uvh Nessus-5.2.4-fc16.x86_64.rpm</code>

Nach Abschluss des Upgrades starten Sie den Dienst <code>nessusd</code> mit dem folgenden Befehl neu:

<code># service nessusd start</code></td></tr>
<tr><td>Beispielausgabe</td><td><code># service nessusd stop</code>
<code>Shutting down Nessus services: [OK]</code>
<code># rpm -Uvh Nessus-5.2.4-fc16.i386.rpm</code>

<code>[..]</code>

<code># service nessusd start</code>
<code>Starting Nessus services: [OK]</code>
<code>#</code></td></tr>
<tr><th colspan="2">SuSE 10 (64-Bit), 11 (32- und 64-Bit)</th></tr>
<tr><td>Upgradebefehle</td><td><code># service nessusd stop</code>

Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete SuSE-Version:

<code># rpm -Uvh Nessus-5.2.4-suse10.x86_64.rpm</code>
<code># rpm -Uvh Nessus-5.2.4-suse11.i586.rpm</code>
<code># rpm -Uvh Nessus-5.2.4-suse11.x86_64.rpm</code>

Nach Abschluss des Upgrades starten Sie den Dienst <code>nessusd</code> mit dem folgenden Befehl neu:

<code># service nessusd start</code></td></tr>
<tr><td>Beispielausgabe</td><td><code># service nessusd stop</code>
<code>Shutting down Nessus services: [OK]</code>
<code># rpm -Uvh Nessus-5.2.4-suse11.i586.rpm</code>
<code>Preparing...</code>

<code>[..]</code>

<code># service nessusd start</code>
<code>Starting Nessus services: [OK]</code>
<code>#</code></td></tr>
</table>

Debian 6 (32- und 64-Bit)	
Upgradebefehle	# **/etc/init.d/nessusd stop** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Debian-Version: # **dpkg -i Nessus-5.2.4-debian6_i386.deb** # **dpkg -i Nessus-5.2.4-debian6_amd64.deb** # **/etc/init.d/nessusd start**
Beispielausgabe	# **/etc/init.d/nessusd stop** # **dpkg -i Nessus-5.2.4-debian6_i386.deb** (Reading database ... 19831 files and directories currently installed.) Preparing to replace nessus 5.2.3 (using Nessus-5.2.4-debian6_i386.deb) ... [..] # **/etc/init.d/nessusd start** Starting Nessus : . #
Ubuntu 10.04 (Paket 9.10), 11.10, 12.04 und 12.10 (i386 und x86-64)	
Upgradebefehle	# **/etc/init.d/nessusd stop** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Ubuntu-Version: # **dpkg -i Nessus-5.2.4-ubuntu910_i386.deb** # **dpkg -i Nessus-5.2.4-ubuntu910_amd64.deb** # **dpkg -i Nessus-5.2.4-ubuntu1110_i386.deb** # **dpkg -i Nessus-5.2.4-ubuntu1110_amd64.deb** # **/etc/init.d/nessusd start**
Beispielausgabe	# **/etc/init.d/nessusd stop** # **dpkg -i Nessus-5.2.4-ubuntu1110_i386.deb** (Reading database ... 19831 files and directories currently installed.) Preparing to replace nessus 5.2.3 (using Nessus-5.2.4-ubuntu1110_i386.deb) ... [..] # **/etc/init.d/nessusd start** Starting Nessus : . #

FreeBSD 9 (32- und 64-Bit)	
Upgradebefehle	# **killall nessusd** # **pkg_info** Durch diesen Befehl wird eine Liste aller installierten Pakete und ihrer Beschreibungen erstellt. Nachfolgend gezeigt ist eine Beispielausgabe für den vorherigen Befehl, der das Nessus-Paket anzeigt: `Nessus-5.2.3        A powerful security scanner` Entfernen Sie das Nessus-Paket mithilfe des folgenden Befehls: # **pkg_delete <Paketname>** Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete FreeBSD-Version: # **pkg_add Nessus-5.2.4-fbsd9.tbz** # **pkg_add Nessus-5.2.4-fbsd9.amd64.tbz** # **/usr/local/nessus/sbin/nessusd -D**
Beispielausgabe	# **killall nessusd** # **pkg_delete Nessus-5.2.3** # **pkg_add Nessus-5.2.4-fbsd9.tbz** nessusd (Nessus) 5.2.4. for FreeBSD (C) 2013 Tenable Network Security, Inc. [..] # **/usr/local/nessus/sbin/nessusd -D** nessusd (Nessus) 5.2.4. for FreeBSD (C) 2013 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded #
Hinweise	Zur Aktualisierung von Nessus unter FreeBSD müssen Sie die vorhandene Version zunächst deinstallieren und dann das neueste Release installieren. Bei diesem Vorgang werden die Konfigurationsdateien sowie Dateien, die nicht Bestandteil der Ursprungsinstallation waren, nicht entfernt.

Installation

Laden Sie die aktuelle Nessus-Version von http://www.tenable.com/products/nessus/select-your-operating-system oder über das Tenable Support Portal herunter. Überprüfen Sie die Integrität des Installationspakets. Hierzu vergleichen Sie die MD5-Prüfsumme der heruntergeladenen Datei mit der in der Datei **`MD5.asc`** (hier) angegebenen Prüfsumme.



Sofern nicht anders angegeben, müssen alle Befehle als Benutzer `root` des Systems ausgeführt werden. Normale Benutzerkonten verfügen gewöhnlich nicht über die zur Installation dieser Software erforderlichen

Berechtigungen.

In der folgenden Tabelle finden Sie Hinweise zur Installation des Nessus-Servers auf allen unterstützten Plattformen. Spezielle Installationshinweise finden Sie jeweils in einer auf das Beispiel folgenden Anmerkung.

Plattform	**Installationsanleitung**
Red Hat ES 4 und CentOS 4 (32-Bit); Red Hat ES 5, CentOS 5 und Oracle Linux 5 (32- und 64-Bit); Red Hat ES 6, CentOS 6 und Oracle Linux 6 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Red Hat-Version: # **rpm -ivh Nessus-5.2.4-es4.i386.rpm** # **rpm -ivh Nessus-5.2.4-es5.i386.rpm** # **rpm -ivh Nessus-5.2.4-es5.x86_64.rpm** # **rpm -ivh Nessus-5.2.4-es6.i686.rpm** # **rpm -ivh Nessus-5.2.4-es6.x86_64.rpm**
Beispielausgabe	# **rpm -ivh Nessus-5.2.4-es4.i386.rpm** Preparing... ### [100%] 1:Nessus ### [100%] nessusd (Nessus) 5.2.4 [build R23011] for Linux (C) 1998 - 2013 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - You can start nessusd by typing /sbin/service nessusd start - Then go to https://localhost:8834/ to configure your scanner #
Fedora Core 16, 17 und 18 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Fedora Core-Version: # **rpm -ivh Nessus-5.2.4-fc16.i686.rpm** # **rpm -ivh Nessus-5.2.4-fc16.x86_64.rpm**
Beispielausgabe	# **rpm -ivh Nessus-5.2.4-fc16.i386.rpm** Preparing... [..] #
SuSE 10 (64-Bit), 11 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete SuSE-Version: # **rpm -ivh Nessus-5.2.4-suse10.x86_64.rpm**

	# **rpm -ivh Nessus-5.2.4-suse11.i586.rpm** # **rpm -ivh Nessus-5.2.4-suse11.x86_64.rpm**

Beispielausgabe	# **rpm -ivh Nessus-5.2.4-suse11.i586.rpm**
	`Preparing...################################### [100%]`
	`   1:Nessus ################################### [100%]`
	
	`[..]`
	
	`#`

Debian 6 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Debian-Version: # **dpkg -i Nessus-5.2.4 -debian6_i386.deb** # **dpkg -i Nessus-5.2.4 -debian6_amd64.deb**

Beispielausgabe	# **dpkg -i Nessus-5.2.4-debian6_i386.deb**
	`Selecting previously deselected package nessus.`
	`(Reading database ... 36954 files and directories currently installed.)`
	`Unpacking nessus (from Nessus-5.2.4-debian6_i386.deb) ...`
	`Setting up nessus (5.2.4) ...`
	
	`[..]`
	
	`#`

Ubuntu 10.04 (Paket 9.10), 11.10, 12.04 und 12.10 (i386 und x86-64)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete Ubuntu-Version: # **dpkg -i Nessus-5.2.4-ubuntu910_i386.deb** # **dpkg -i Nessus-5.2.4-ubuntu910_amd64.deb** # **dpkg -i Nessus-5.2.4-ubuntu1110_i386.deb** # **dpkg -i Nessus-5.2.4-ubuntu1110_amd64.deb**

Beispielausgabe	# **dpkg -i Nessus-5.2.4-ubuntu1110_amd64.deb**
	`Selecting previously deselected package nessus.`
	`(Reading database ... 32444 files and directories currently installed.)`
	`Unpacking nessus (from Nessus-5.2.4-ubuntu1110_amd64.deb) ...`
	`Setting up nessus (5.2.4) ...`
	
	`[..]`
	`#`

FreeBSD 9 (32- und 64-Bit)	
Installationsbefehl	Verwenden Sie den passenden der nachfolgend aufgeführten Befehle für die von Ihnen verwendete FreeBSD-Version: # **pkg_add Nessus-5.2.4-fbsd9.tbz**

	`# pkg_add Nessus-5.2.4-fbsd9.amd64.tbz`

Beispielausgabe	`# pkg_add Nessus-5.2.4-fbsd9.tbz`
	
	`nessusd (Nessus) 5.2.4 for FreeBSD`
	`(C) 1998 - 2013 Tenable Network Security, Inc.`
	
	`[..]`
	`#`

Nach Abschluss der Installation starten Sie den Daemon **nessusd** wie im nächsten Abschnitt für Ihre Distribution beschrieben. Nach der Installation von Nessus müssen Sie die angegebene Scanner-URL besuchen, um die Registrierung durchzuführen.



Hinweis: Bei Installationen auf UNIX-Basis wird unter Umständen eine URL angegeben, die einen relativen, nicht im DNS enthaltenen Hostnamen (z. B. https://myserver:8834/) enthält. Ist der Hostname nicht im DNS vorhanden, dann müssen Sie die Verbindung zum Nessus-Server über eine IP-Adresse oder einen gültigen DNS-Namen herstellen.

Nach Abschluss der Installation werden eine Authentifizierung und die Anpassung der Konfigurationsoptionen an Ihre Umgebung empfohlen. Eine Beschreibung hierzu finden Sie im Abschnitt „Feed registrieren und Benutzeroberfläche konfigurieren“.



Nessus muss auf **/opt/nessus** installiert werden. Ein Symlink (symbolische Verknüpfung) mit **/opt/nessus** wird ebenfalls angenommen.

Den Nessus-Daemon starten

Starten Sie den Nessus-Dienst als `root` mit dem folgenden Befehl:

Linux:
```
# /opt/nessus/sbin/nessus-service -D
```

FreeBSD:
```
# /usr/local/nessus/sbin/nessus-service -D
```

Nachfolgend gezeigt ist eine Beispielausgabe für den Start von **nessusd** unter Red Hat:

```
[root@squirrel ~]# /sbin/service nessusd start
Starting Nessus services:                                    [ OK ]
[root@squirrel ~]#
```

Wenn Sie die Ausgabe des Befehls unterdrücken möchten, verwenden Sie die Option `-q` wie folgt:

Linux:
```
# /opt/nessus/sbin/nessus-service -q -D
```

FreeBSD:
```
# /usr/local/nessus/sbin/nessus-service -q -D
```

Alternativ kann Nessus abhängig von der Betriebssystemplattform mit dem folgenden Befehl gestartet werden:

Betriebssystem	Startbefehl für `nessusd`
Red Hat, CentOS, & Oracle Linux	`# /sbin/service nessusd start`
Fedora Core	`# /sbin/service nessusd start`
SuSE	`# /etc/rc.d/nessusd start`
Debian	`# /etc/init.d/nessusd start`
FreeBSD	`# /usr/local/etc/rc.d/nessusd.sh start`
Ubuntu	`# /etc/init.d/nessusd start`

Fahren Sie fort wie im Abschnitt „Feed registrieren und Benutzeroberfläche konfigurieren“ beschrieben, um den Plugin-Aktivierungscode zu installieren.

Den Nessus-Daemon beenden

Wenn Sie den Dienst **nessusd** aus irgendeinem Grund beenden müssen, verwenden Sie den folgenden Befehl, um Nessus anzuhalten **und alle laufenden Scans direkt zu beenden**:

```
# killall nessusd
```

Wir empfehlen jedoch, stattdessen die folgenden von Ihrem Betriebssystem bereitgestellten, weniger drastisch agierenden Skripts zum Beenden zu verwenden:

Betriebssystem	Stoppbefehl für `nessusd`
Red Hat, CentOS, & Oracle Linux	`# /sbin/service nessusd stop`
Fedora Core	`# /sbin/service nessusd stop`
SuSE	`# /etc/rc.d/nessusd stop`
Debian	`# /etc/init.d/nessusd stop`
FreeBSD	`# /usr/local/etc/rc.d/nessusd.sh stop`
Ubuntu	`# /etc/init.d/nessusd stop`

Nessus entfernen

In der folgenden Tabelle finden Sie Hinweise zum Entfernen des Nessus-Servers auf allen unterstützten Plattformen. Mit Ausnahme von Mac OS X werden bei diesem Vorgang weder Konfigurationsdateien noch Dateien entfernt, die nicht Bestandteil der Ursprungsinstallation waren. Dateien, die Bestandteil des Originalpakets waren, aber seit der Installation

geändert wurden, werden ebenfalls nicht entfernt. Zur Entfernung der übrigen Dateien verwenden Sie den folgenden Befehl:

Linux:
```
# rm -rf /opt/nessus
```

FreeBSD:
```
# rm -rf /usr/local/nessus/bin
```

Plattform	Deinstallationsanleitung
Red Hat ES 4 und CentOS 4 (32-Bit); Red Hat ES 5, CentOS 5 und Oracle Linux 5 (32- und 64-Bit); Red Hat ES 6, CentOS 6 und Oracle Linux 6 (32- und 64-Bit)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: `# rpm -qa	grep Nessus`  Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen:  `# rpm -e <Paketname>`
Beispielausgabe	`# rpm -qa	grep -i nessus` `Nessus-5.2.4-es5` `# rpm -e Nessus-5.2.4-es5` `#`
Fedora Core 16, 17 und 18 (32- und 64-Bit)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: `# rpm -qa	grep Nessus`  Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen:  `# rpm -e <Paketname>`
SuSE 10 (64-Bit), 11 (32- und 64-Bit)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: `# rpm -qa	grep Nessus`  Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen:  `# rpm -e <Paketname>`
Debian 6 (32- und 64-Bit)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: `# dpkg -l	grep -i nessus` Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen:

	# **dpkg -r <Paketname>**
Beispielausgabe	# **dpkg -l | grep nessus** ii nessus 5.2.4 Version 5 of the Nessus Scanner # **dpkg -r nessus** #
Ubuntu 10.04 (Paket 9.10), 11.10, 12.04 und 12.10 (i386 und x86-64)	
Deinstallationsbefehl	Ermitteln Sie den Paketnamen: # **dpkg -l | grep -i nessus** Verwenden Sie die Ausgabe des obigen Befehls, um das Paket zu entfernen: # **dpkg -r <Paketname>**
Beispielausgabe	# **dpkg -l | grep -i nessus** ii nessus 5.2.4 Version 5 of the Nessus Scanner #
FreeBSD 9 (32- und 64-Bit)	
Deinstallationsbefehl	Beenden Sie Nessus: # **killall nessusd** Ermitteln Sie den Paketnamen: # **pkg_info | grep -i nessus** Entfernen Sie das Nessus-Paket: # **pkg_delete <Paketname>**
Beispielausgabe	# **killall nessusd** # **pkg_info | grep -i nessus** Nessus-5.2.4 A powerful security scanner # **pkg_delete Nessus-5.2.4** #

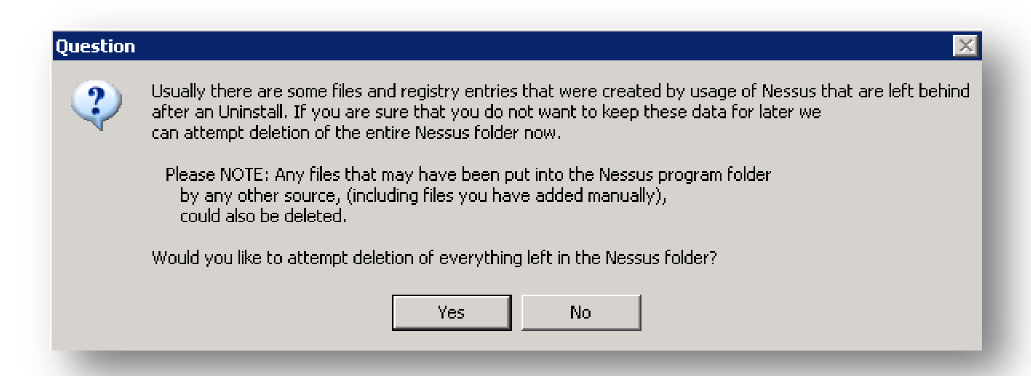
Windows

Upgrade ausführen

Das Upgrade von Nessus 5.x auf eine neuere 5.x Version ist unkompliziert und erfordert keinerlei weiteren Erwägungen.

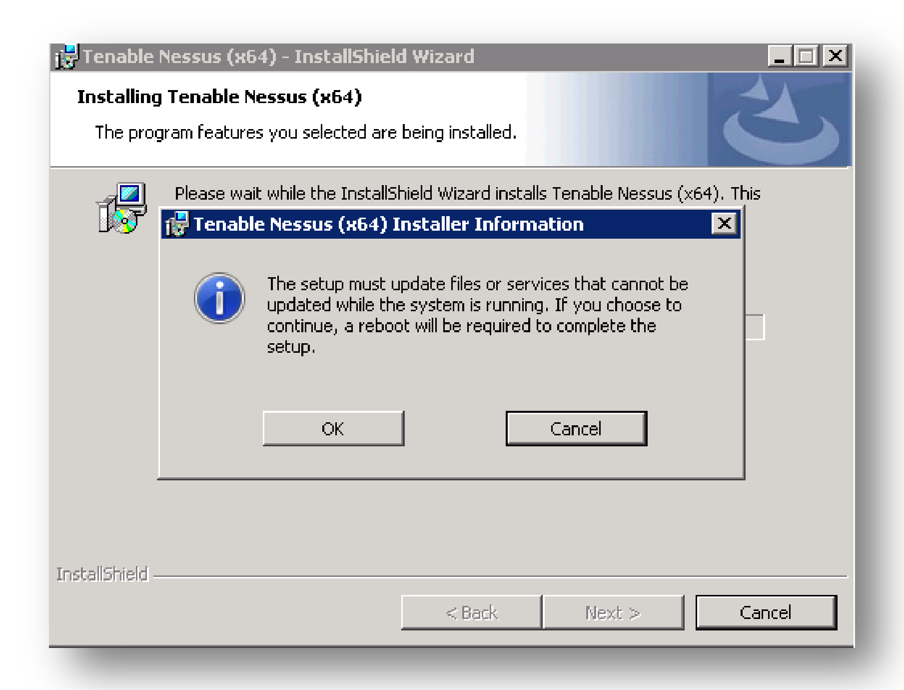
Upgrade von Nessus 4.x ausführen

Beim Nessus-Upgrade von einer Version 4.x auf eine neuere 5.x-Distribution werden Sie im Verlauf des Upgrade-vorgangs gefragt, ob Sie den gesamten Inhalt des Nessus-Verzeichnisses löschen möchten. Wenn Sie sich für diese Option entscheiden (indem Sie „Yes“ auswählen), wird ein Deinstallationsprozess imitiert. In diesem Fall werden zuvor erstellte Benutzer, vorhandene Scanrichtlinien und Scanergebnisse entfernt, und die Registrierung des Scanners wird aufgehoben.



Klicken Sie auf „Yes" („Ja"), wenn Nessus versuchen soll, den gesamten Nessus-Ordner sowie ggf. manuell hinzugefügte Dateien zu löschen, oder auf „No" („Nein"), wenn der Nessus-Ordner sowie die vorhandenen Scans, Berichte usw. beibehalten werden sollen. Nach der Installation der neuen Nessus-Version stehen diese weiterhin für Ansicht und Export zur Verfügung.

Abhängig von der gegenwärtig installierten und der neu zu installierenden Version werden Sie möglicherweise aufgefordert, einen Neustart durchzuführen:



Upgrade von Nessus 3.x ausführen

Ein direktes Upgrade von Nessus 3.0.x auf Nessus 5.x wird nicht unterstützt. Sie können allerdings als Zwischenschritt ein Upgrade auf Version 4 durchführen, um sicherzustellen, dass wichtige Scaneinstellungen und -richtlinien nicht verloren gehen. Wenn Sie die Scaneinstellungen nicht behalten möchten, deinstallieren Sie zunächst Nessus 3.x und installieren Sie Nessus 5 dann von Grund auf neu.



Wenn Sie „Yes" („Ja") auswählen, werden alle Dateien im Nessus-Verzeichnis einschließlich der Logdateien, manuell hinzugefügter angepasster Plugins usw. gelöscht. Wählen Sie diese Option nur aus, wenn Sie sich

ganz sicher sind!

Installation

Nessus herunterladen

Die aktuelle Nessus-Version ist auf der Seite http://www.tenable.com/products/nessus/select-your-operating-system oder über das Tenable Support Portal verfügbar. Nessus 5 ist für Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista und Windows 7 erhältlich. Überprüfen Sie die Integrität des Installationspakets. Hierzu vergleichen Sie die MD5-Prüfsumme der heruntergeladenen Datei mit der in der Datei **MD5.asc** (hier) angegebenen Prüfsumme.

Die Größen und Namen von Nessus-Distributionsdateien unterschiedlicher Versionen variieren geringfügig. Im Allgemeinen liegt die Dateigröße jedoch immer bei etwa 25 MB.

Installation

Nessus wird als ausführbare Installationsdatei vertrieben. Speichern Sie die Datei auf dem System, auf dem die Installation ausgeführt werden soll, oder auf einem freigegebenen Laufwerk, auf das vom System aus zugegriffen werden kann.

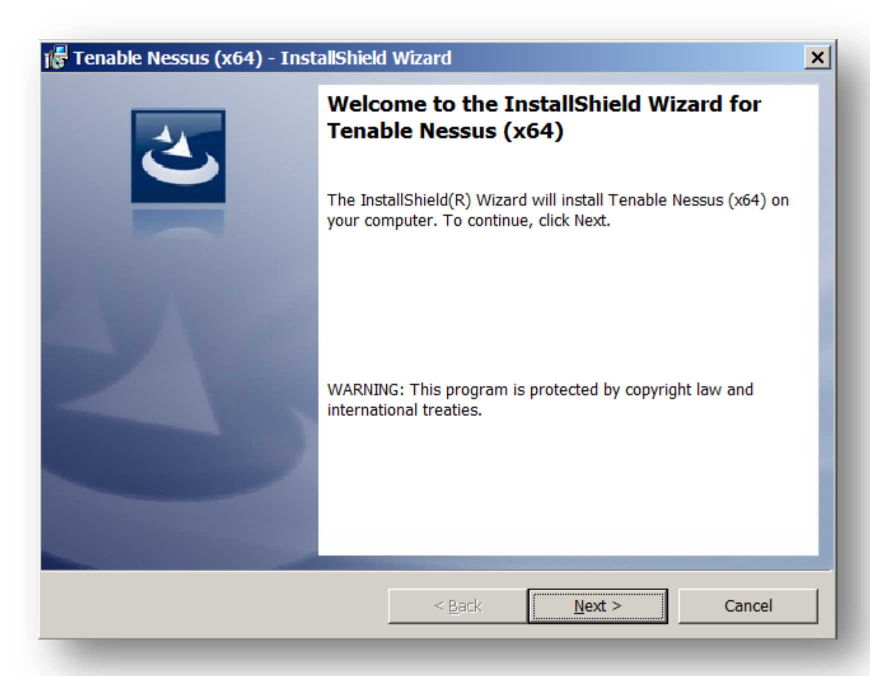
Sie müssen Nessus mit einem Konto mit Administratorrechten installieren; ein normales Benutzerkonto ist nicht ausreichend. Wenn Fehlermeldungen in Bezug auf Berechtigungen, Zugriffsverweigerungen oder Fehler auftreten, die das Fehlen bestimmter Berechtigungen wahrscheinlich machen, stellen Sie sicher, dass Sie ein Konto mit Administratorrechten verwenden. Erhalten Sie diese Fehlermeldungen bei der Verwendung der Befehlszeilen-Utilitys, dann führen Sie **cmd.exe** unter einem ausführenden Konto mit Administratorrechten aus.



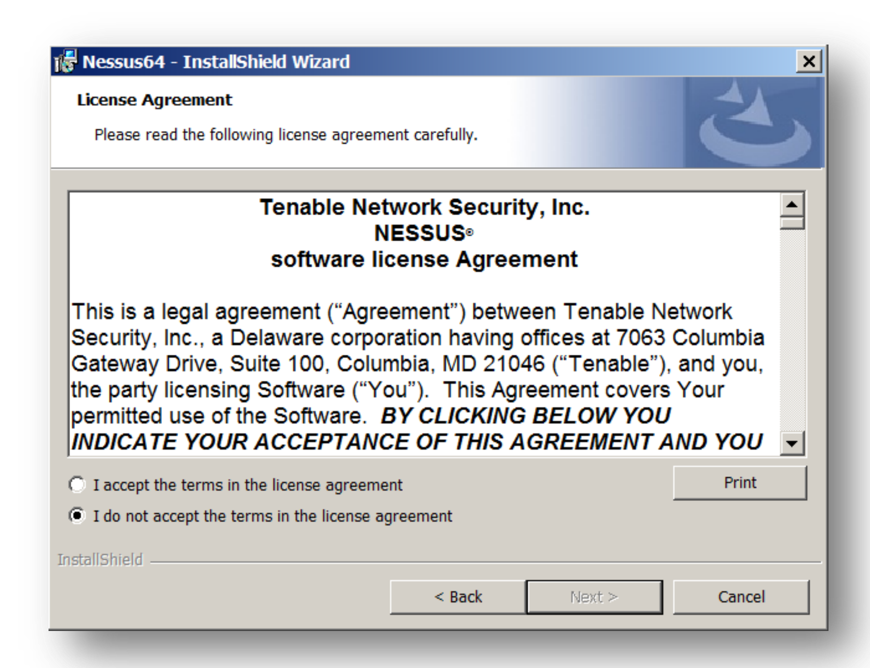
Bestimmte Antivirensoftware kann Nessus möglicherweise als Wurm oder eine andere Form von Schadsoftware klassifizieren. Dies ist durch die große Anzahl der TCP-Verbindungen bedingt, die bei einem Scan erzeugt wird. Wenn Ihre Antivirensoftware eine Warnung ausgibt, klicken Sie auf „Zulassen“, damit der Nessus-Scan fortgesetzt werden kann. Die meisten Antivirenpakete ermöglichen auch das Hinzufügen von Prozessen zu einer Ausnahmeliste. Fügen Sie **Nessus.exe** und **Nessus-service.exe** dieser Liste hinzu, um solche Warnmeldungen in Zukunft zu vermeiden.

Es wird empfohlen, sich vor Beginn des Installationsvorgangs einen Aktivierungscode für Plugin-Feeds zu besorgen, da diese Information benötigt wird, damit Sie sich bei der Nessus-Benutzeroberfläche authentifizieren können. Weitere Informationen zum Bezug eines Aktivierungscodes finden Sie im Abschnitt „Sicherheitslücken-Plugins“.

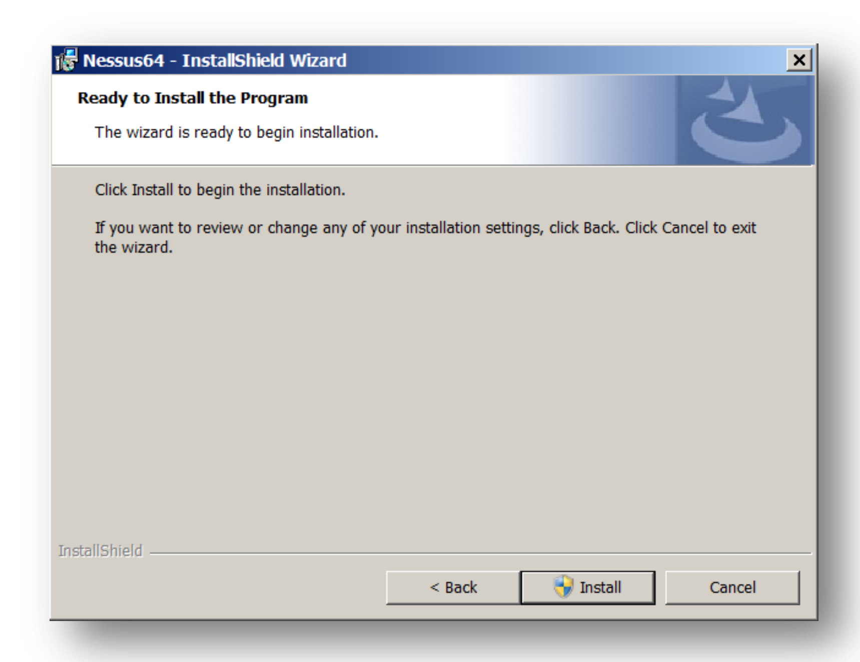
Fragen zur Installation



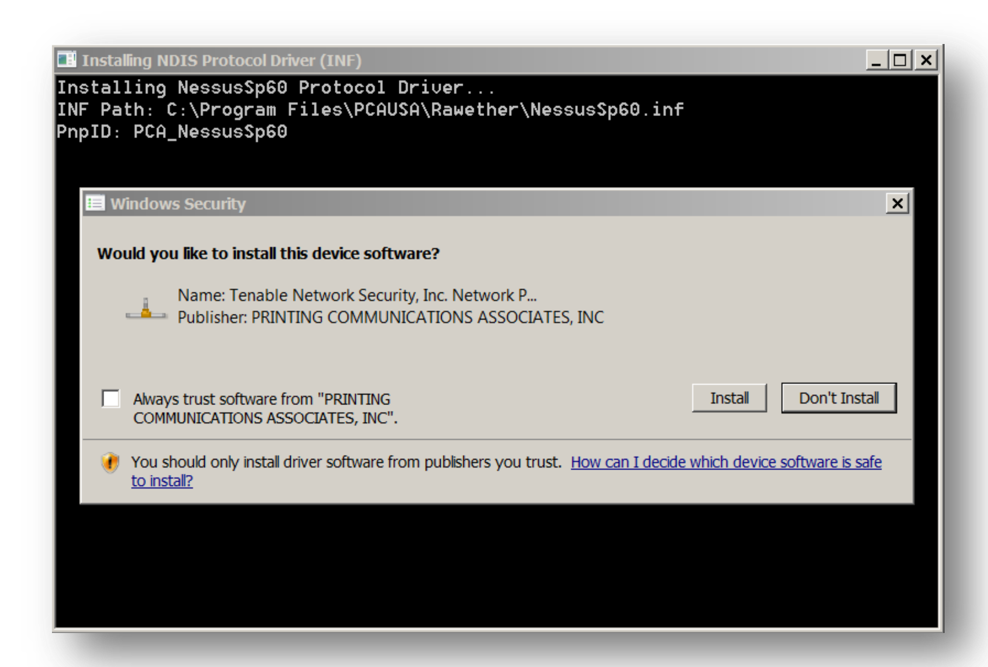
Während des Installationsvorgangs von Nessus werden einige Angaben beim Benutzer erfragt. Zu Beginn müssen Sie den Lizenzvertrag lesen und ihm zustimmen:



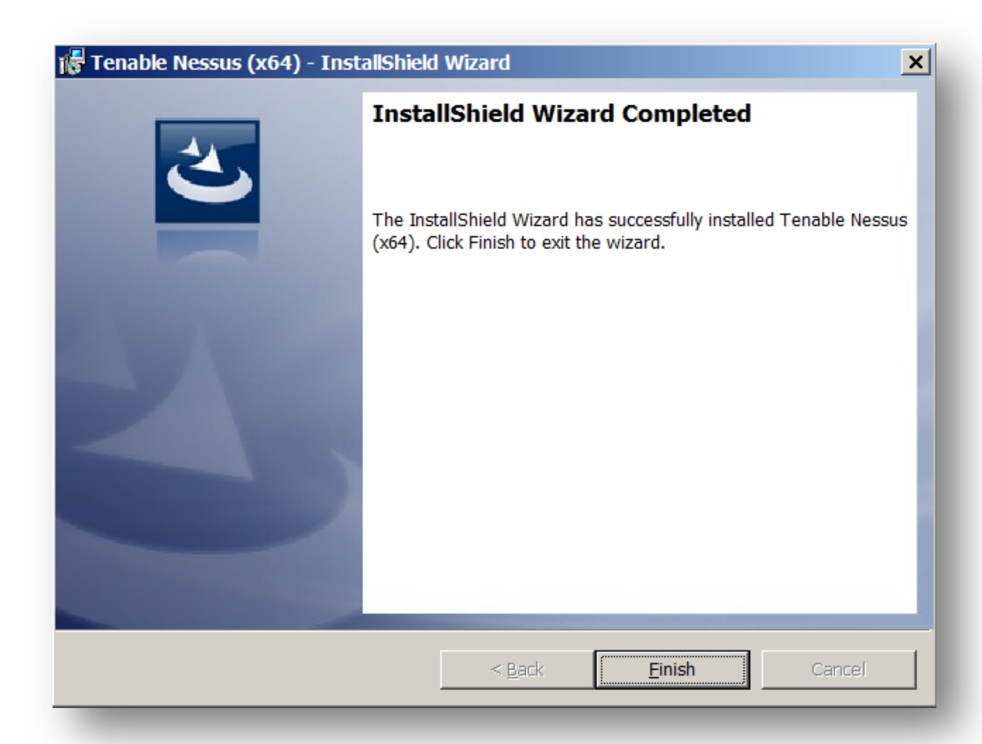
Sie werden nun aufgefordert, die Installation zu bestätigen:



Nach Abschluss der Erstinstallation startet Nessus ggf. die Installation eines Drittanbietertreibers, der zur Unterstützung der Ethernet-Kommunikation von Nessus verwendet wird:



Klicken Sie nach Abschluss der Installation auf „Finish“ („Fertig stellen“).

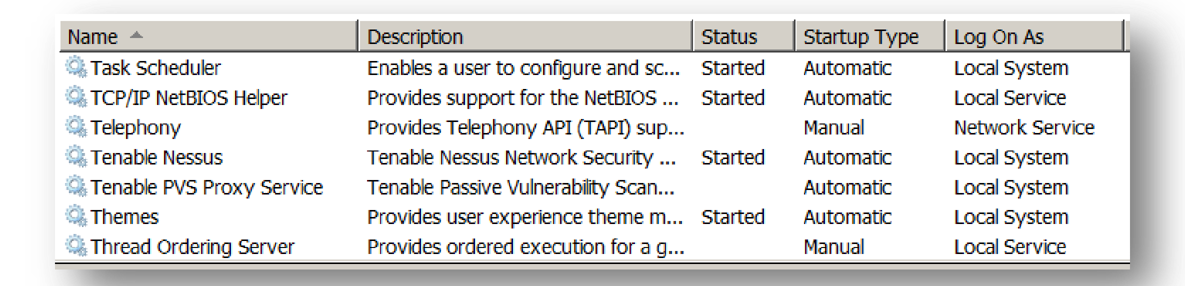


Nun wird von Nessus eine Seite in Ihren Standardwebbrowser geladen, auf der die Erstkonfiguration erledigt wird. Sie wird im Abschnitt „Feed registrieren und Benutzeroberfläche konfigurieren“ behandelt.

Den Nessus-Daemon starten und beenden

Während der Installation und im täglichen Betrieb von Nessus sind Änderungen am Nessus-Dienst in der Regel nicht erforderlich. Es kann jedoch vorkommen, dass Administratoren den Dienst vorübergehend anhalten oder neu starten möchten.

Bei Windows-Systemen öffnen Sie hierzu das Startmenü und klicken auf „Ausführen“. Geben Sie „`services.msc`“ in das Feld „Ausführen“ ein, um den Windows Service Manager zu öffnen:



Name	Description	Status	Startup Type	Log On As
Task Scheduler	Enables a user to configure and sc...	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Provides support for the NetBIOS ...	Started	Automatic	Local Service
Telephony	Provides Telephony API (TAPI) sup...		Manual	Network Service
Tenable Nessus	Tenable Nessus Network Security ...	Started	Automatic	Local System
Tenable PVS Proxy Service	Tenable Passive Vulnerability Scan...		Automatic	Local System
Themes	Provides user experience theme m...	Started	Automatic	Local System
Thread Ordering Server	Provides ordered execution for a g...		Manual	Local Service

Nach einem Rechtsklick auf den Dienst „Tenable Nessus“ wird ein Kontextmenü angezeigt, in dem Sie den Dienst je nach aktuellem Status starten, beenden, anhalten, fortsetzen oder neu starten können.

Der Nessus-Dienst kann außerdem über die Befehlszeile bedient werden. Weitere Informationen finden Sie unter „Nessus-Dienst über die Windows-Befehlszeile steuern“ in diesem Dokument.

Nessus entfernen

Zum Entfernen von Nessus öffnen Sie in der Systemsteuerung den Eintrag „**Software**“. Wählen Sie „**Tenable Nessus**“ aus und klicken Sie dann auf die Schaltfläche „**Ändern/Entfernen**“. Das Fenster „InstallShield Wizard“ („InstallShield-Assistent“) wird geöffnet. Befolgen Sie die Anweisungen im Assistenten, um Nessus vollständig zu entfernen. Sie werden aufgefordert, anzugeben, ob Sie den gesamten Nessus-Ordner entfernen möchten. Wählen Sie „Yes“ nur dann aus, wenn Sie keine zuvor generierten Scanergebnisse und -richtlinien behalten möchten.



Bei der Deinstallation werden Sie gefragt, ob Sie fortfahren möchten, da die angegebene **`.msi`**-Datei unsigniert ist. Beispiel:

C:\Windows\Installer\778608.msi
Herausgeber: unbekannt

Ursache hierfür ist, dass Windows eine interne Kopie des Nessus-Installationsprogramms speichert und diese dann zum Starten des Deinstallationsvorgangs verwendet. Sie können diese Anfrage deswegen beruhigt bestätigen.

Mac OS X

Upgrade ausführen

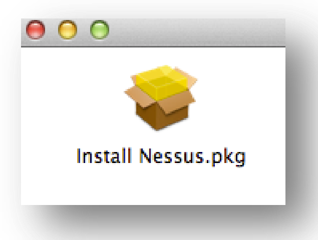
Das Upgrade von einer älteren Nessus-Version entspricht einer Neuinstallation. Laden Sie die Datei **`Nessus-5.x.x.dmg.gz`** herunter und doppelklicken Sie darauf, um sie zu entpacken. Doppelklicken Sie dann auf die Datei **`Nessus-5.x.x.dmg`**. Mithilfe dieser Datei wird das Image aktiviert und unter „Geräte“ im Finder aufgeführt. Sobald das Volume „Nessus 5“ im Finder angezeigt wird, doppelklicken Sie auf die Datei „Nessus 5“. Melden Sie sich nach Abschluss der Installation bei Nessus an, indem Sie in Ihrem Browser die Adresse https://localhost:8834 aufrufen.

Installation

Die aktuelle Nessus-Version ist auf der Seite http://www.tenable.com/products/nessus/select-your-operating-system oder über das Tenable Support Portal verfügbar. Nessus ist für Mac OS X 10.8 und 10.9 erhältlich. Überprüfen Sie die Integrität des Installationspakets. Hierzu vergleichen Sie die MD5-Prüfsumme der heruntergeladenen Datei mit der in der Datei **`MD5.asc`** (hier) angegebenen Prüfsumme.

Die Größen der Nessus-Distributionsdateien unterschiedlicher Versionen für Mac OS X variieren geringfügig. Im Allgemeinen liegt die Dateigröße jedoch immer bei etwa 45 MB.

Zur Installation von Nessus unter Mac OS X laden Sie die Datei **`Nessus-5.x.x.dmg.gz`** herunter und doppelklicken darauf, um sie zu entpacken. Doppelklicken Sie dann auf die Datei **`Nessus-5.x.x.dmg`**. Mithilfe dieser Datei wird das Image aktiviert und unter „Geräte“ im Finder aufgeführt. Wenn das Volume „Nessus 5“ im Finder angezeigt wird, doppelklicken Sie auf die Datei **`Nessus 5`**:

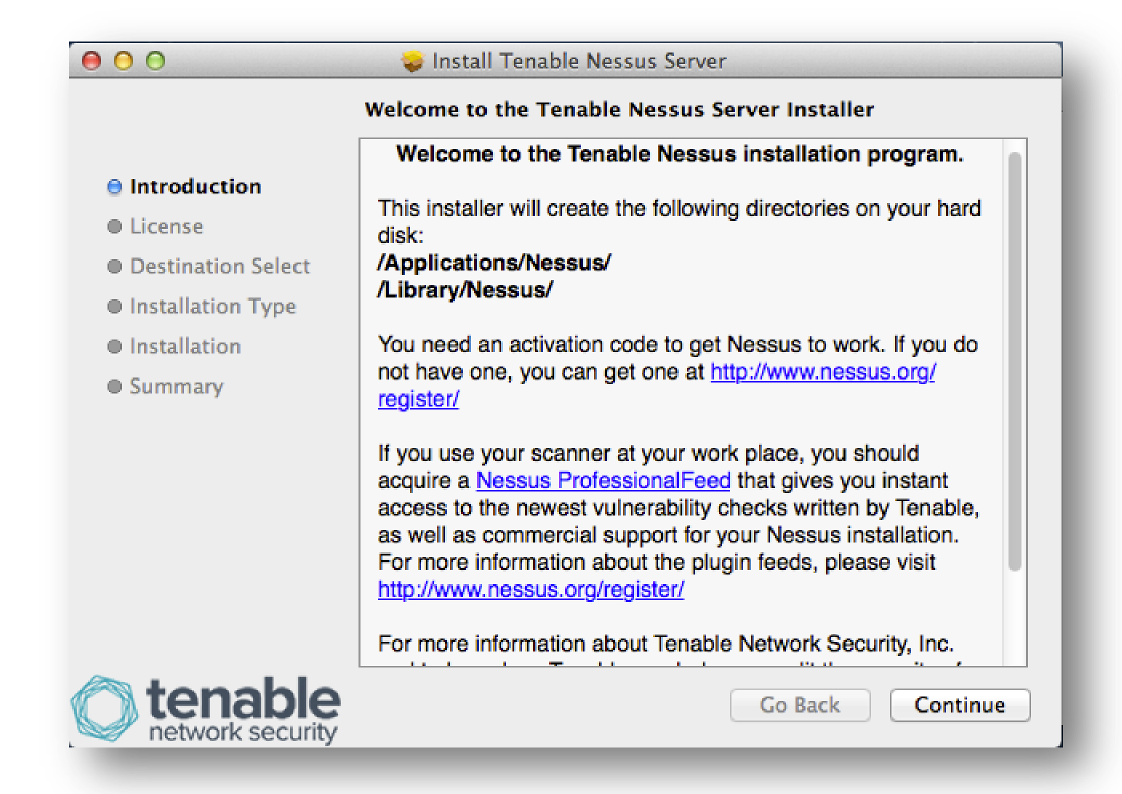




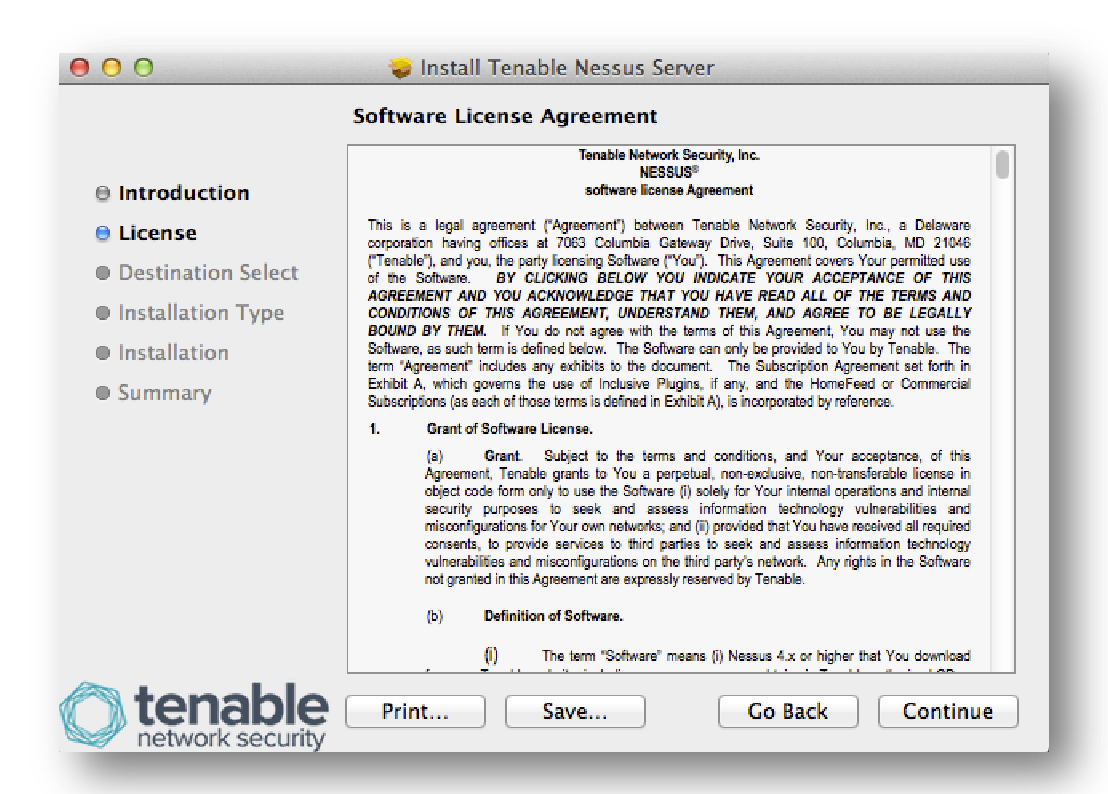
Beachten Sie, dass Sie während der Installation zur Eingabe des Benutzernamens und Kennworts des Administrators aufgefordert werden.

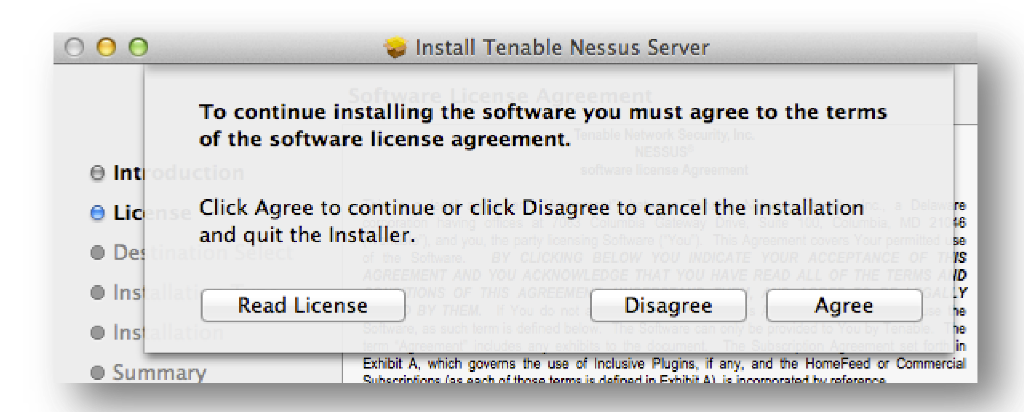
Fragen zur Installation

Die Installation wird wie folgt angezeigt:

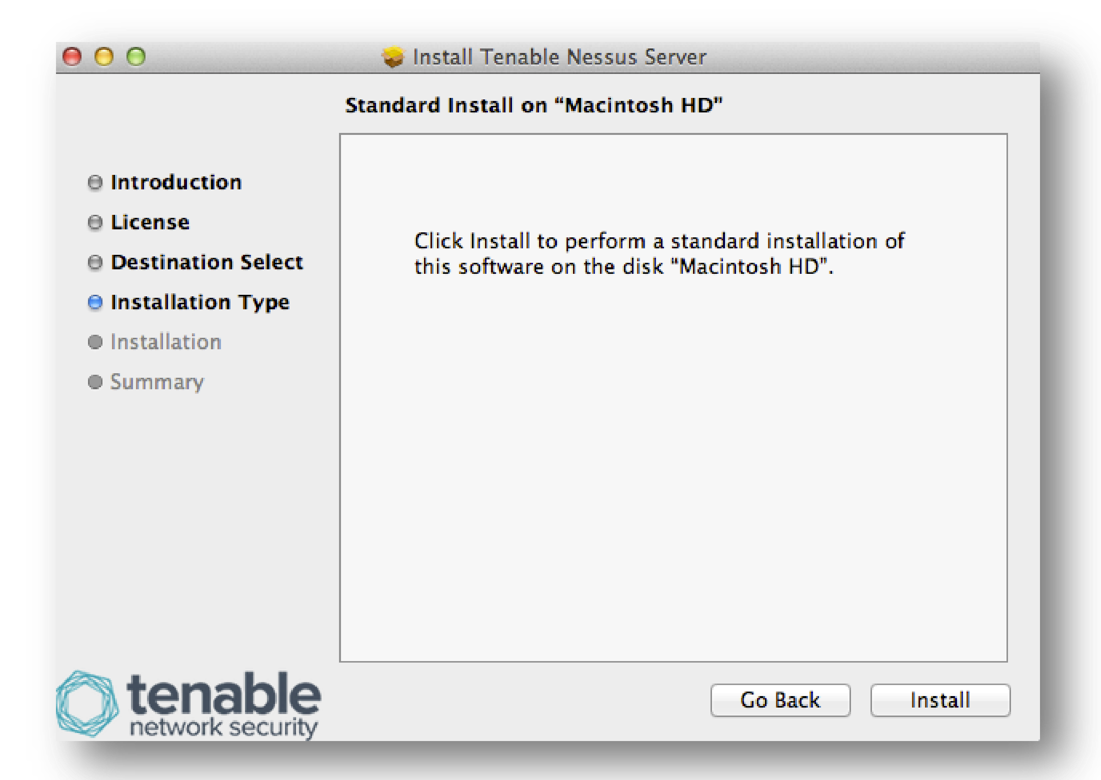


Klicken Sie auf „Continue“ („Weiter“), um die Softwarelizenz anzuzeigen. Klicken Sie erneut auf „Continue“. Nun erscheint ein Dialogfeld, in dem Sie die Lizenzbedingungen akzeptieren müssen, um fortfahren zu können:

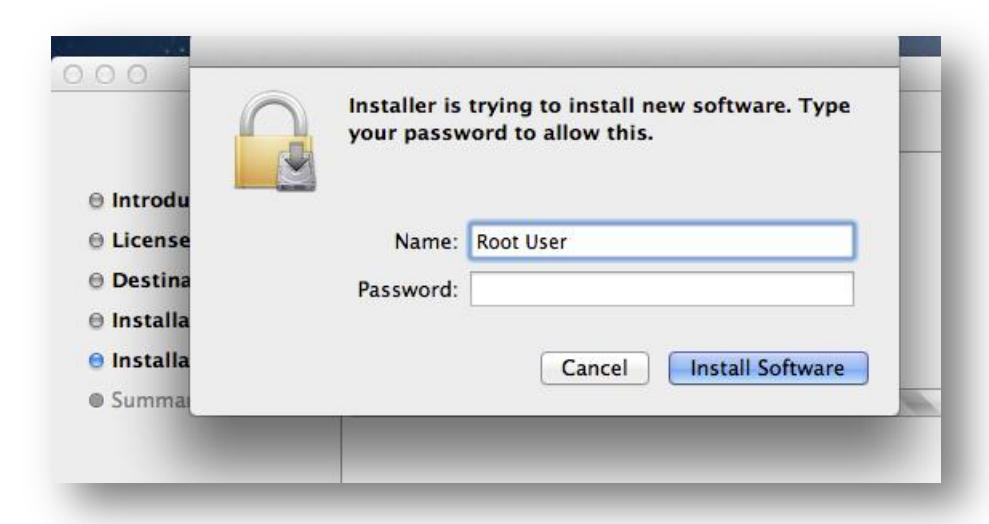




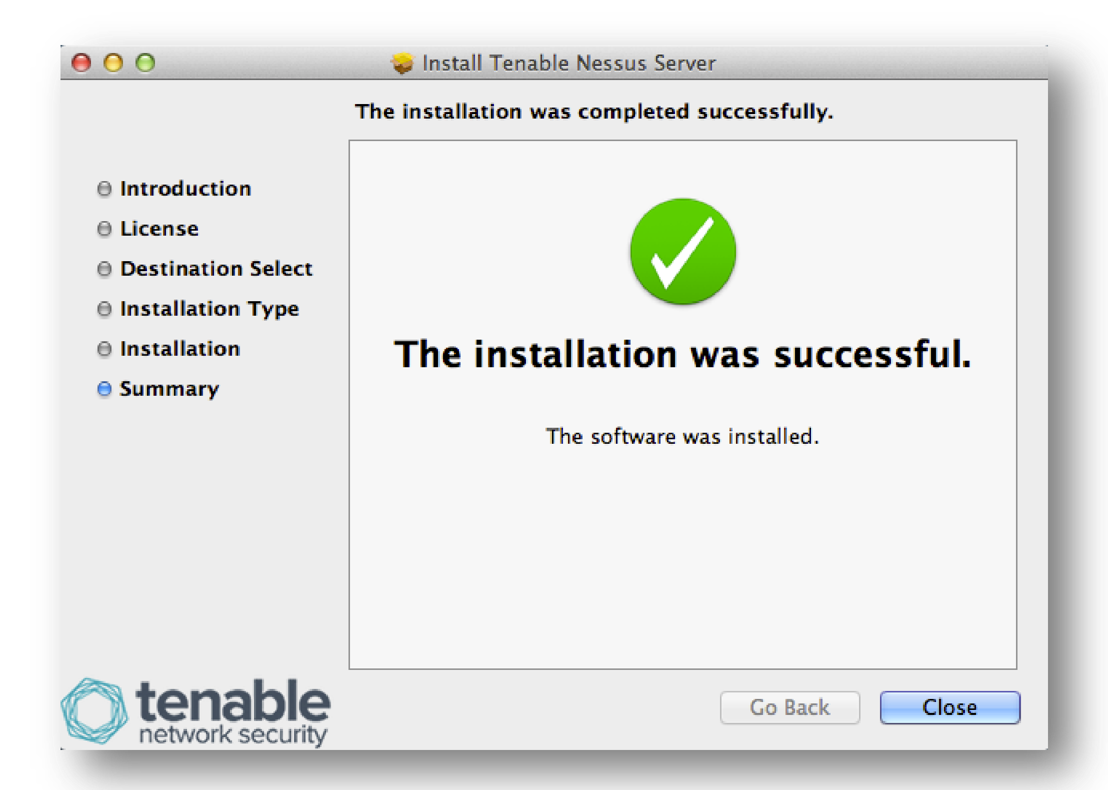
Nach dem Akzeptieren der Lizenz erscheint ein weiteres Dialogfeld, in dem Sie den vorgegebenen Installationsort wie gezeigt ändern können:



Klicken Sie auf „Install“ („Installieren“), um die Installation fortzusetzen. Sie werden nun aufgefordert, Benutzernamen und Kennwort des Administrators einzugeben:



Die Installation wurde erfolgreich abgeschlossen, wenn das folgende Fenster angezeigt wird:



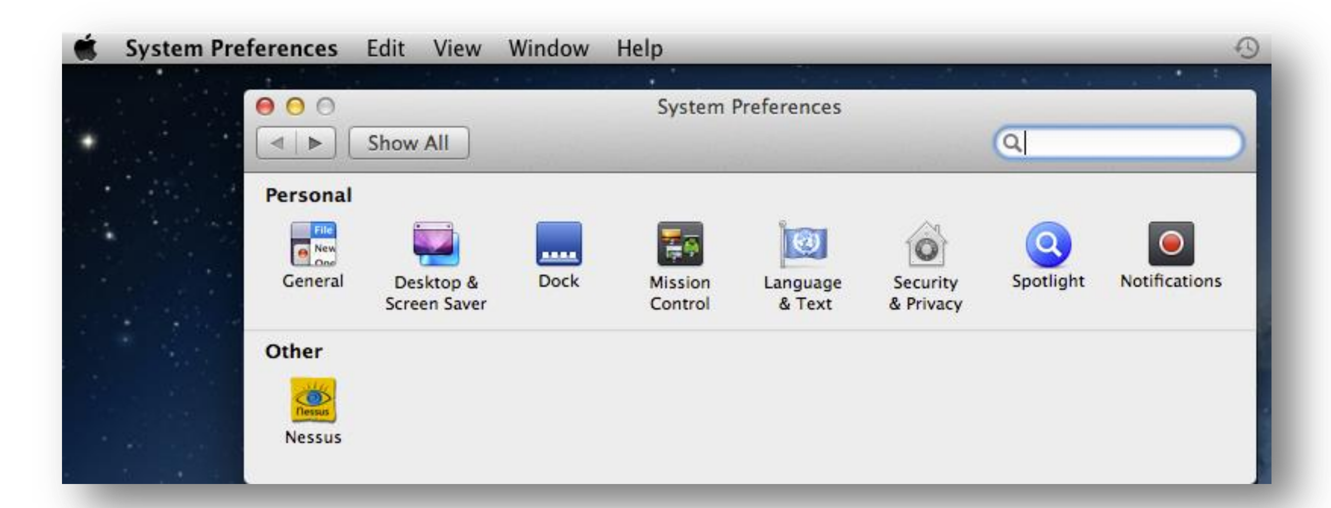
Nun wird von Nessus eine Seite in Ihren Standardwebbrowser geladen, auf der die Erstkonfiguration erledigt wird. Sie wird im Abschnitt „Feed registrieren und Benutzeroberfläche konfigurieren" behandelt.

Nessus-Dienst starten und beenden

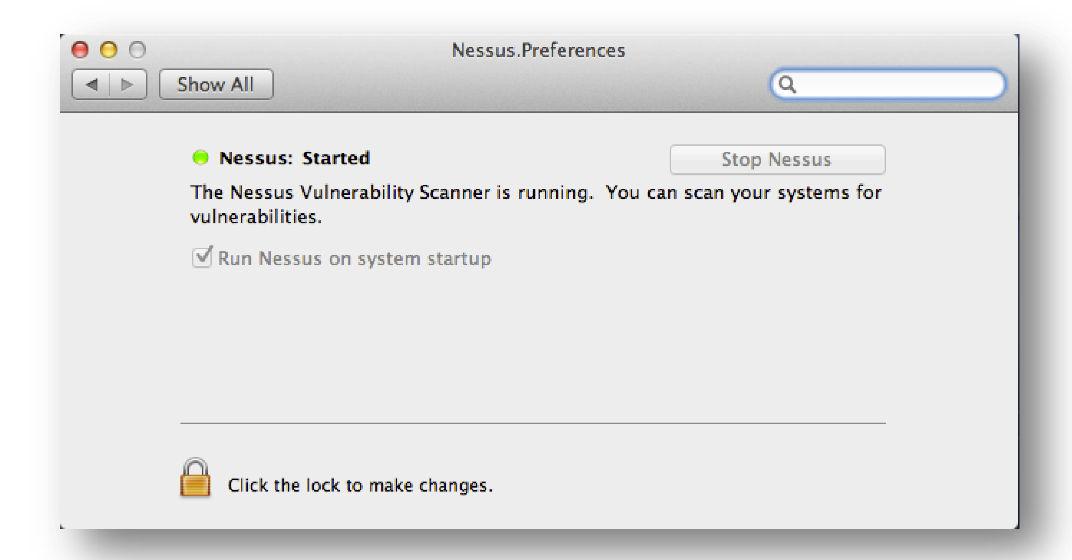
Nach der Installation wird der Dienst **nessusd** gestartet. Der Dienst wird von nun an bei jedem Neustart automatisch gestartet. Falls es notwendig sein sollte, den Dienst zu starten oder zu beenden, können Sie dies über ein Terminal-fenster (Befehlszeile) oder über die Systemeinstellungen tun. Der Befehl muss als „root" bzw. über **sudo** ausgeführt werden:

Aktion	nessusd-Verwaltungsbefehl
Starten	`# launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist`
Beenden	`# launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist`

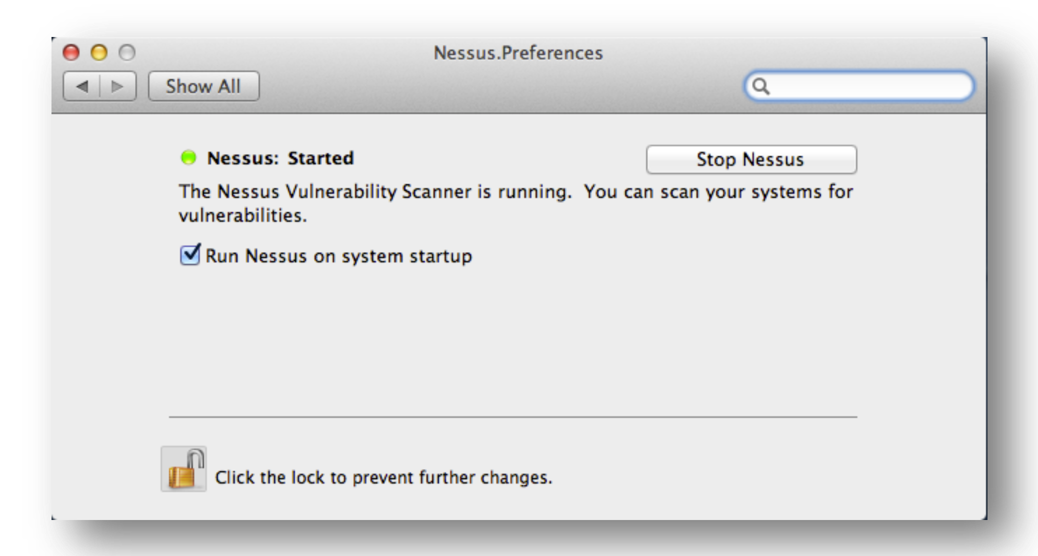
Alternativ dazu kann der Nessus-Dienst über die Systemeinstellungen verwaltet werden:



Klicken Sie in den Systemeinstellungen auf „Nessus“, um das Feld „Nessus.Preferences“ zu laden:



Klicken Sie zur Änderung des Dienststatus auf das Schlosssymbol und geben Sie das Kennwort für „root“ ein. Auf diese Weise können Sie die Starteinstellung im System ändern oder den Nessus-Dienst starten oder beenden:



Nessus entfernen

Löschen Sie zum Entfernen von Nessus die folgenden Verzeichnisse (einschließlich der Unterverzeichnisse) und Dateien:

```
/Library/Receipts/Nessus*/Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
/Library/Nessus
/Library/PreferencePanes/Nessus Preferences.prefPane
/Applications/Nessus
```



Wenn Sie mit der Verwendung der UNIX-Befehlszeile auf einem Mac OS X-System nicht vertraut sind, wenden Sie sich an den Tenable-Support, um Unterstützung zu erhalten.

Es gibt Freewaretools wie „DesInstaller.app“ (http://www.macupdate.com/info.php/id/7511) und „CleanApp“ (http://www.macupdate.com/info.php/id/21453/cleanapp), die ebenfalls zum Entfernen von Nessus verwendet werden können. Tenable steht in keinerlei Abhängigkeitsverhältnis zu den Herstellern oder Vertreibern dieser Tools. Zudem wurden die Tools nicht speziell für die Entfernung von Nessus getestet.

Feed registrieren und Benutzeroberfläche konfigurieren

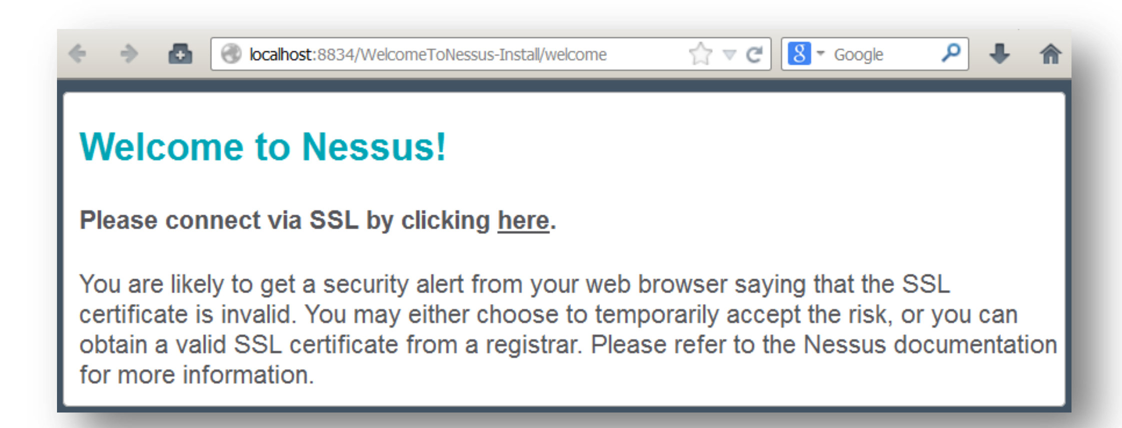
Dieser Abschnitt beschreibt, wie Sie den Nessus 5-Server auf den unterschiedlichen Plattformen konfigurieren. Beginnend mit Nessus 5 erfolgt die Erstkonfiguration beispielsweise von Proxyoptionen und Aktivierungscode im Rahmen eines webbasierten Vorgangs. Nach der Installation von Nessus haben Sie aus Sicherheitsgründen sechs Stunden Zeit, den Registrierungsvorgang durchzuführen. Wird die Registrierung in diesem Zeitraum nicht abgeschlossen, dann starten Sie `nessusd` neu und beginnen Sie die Registrierung von vorne.



Der in Nessus 4 verwendete Nessus Server Manager ist nun veraltet.

Wenn die Konfigurationsseite in Ihrem Browser nach der Softwareinstallation nicht geöffnet wird, starten Sie den Browser und rufen Sie die Adresse http://[Nessus Server IP]:8834/WelcomeToNessus-Install/welcome (bzw. die während des Installationsvorgangs angegebene URL) auf, um den Vorgang zu starten. Hinweis: Bei Installationen auf UNIX-Basis wird unter Umständen eine URL angegeben, die einen relativen, nicht im DNS enthaltenen Hostnamen (z. B.

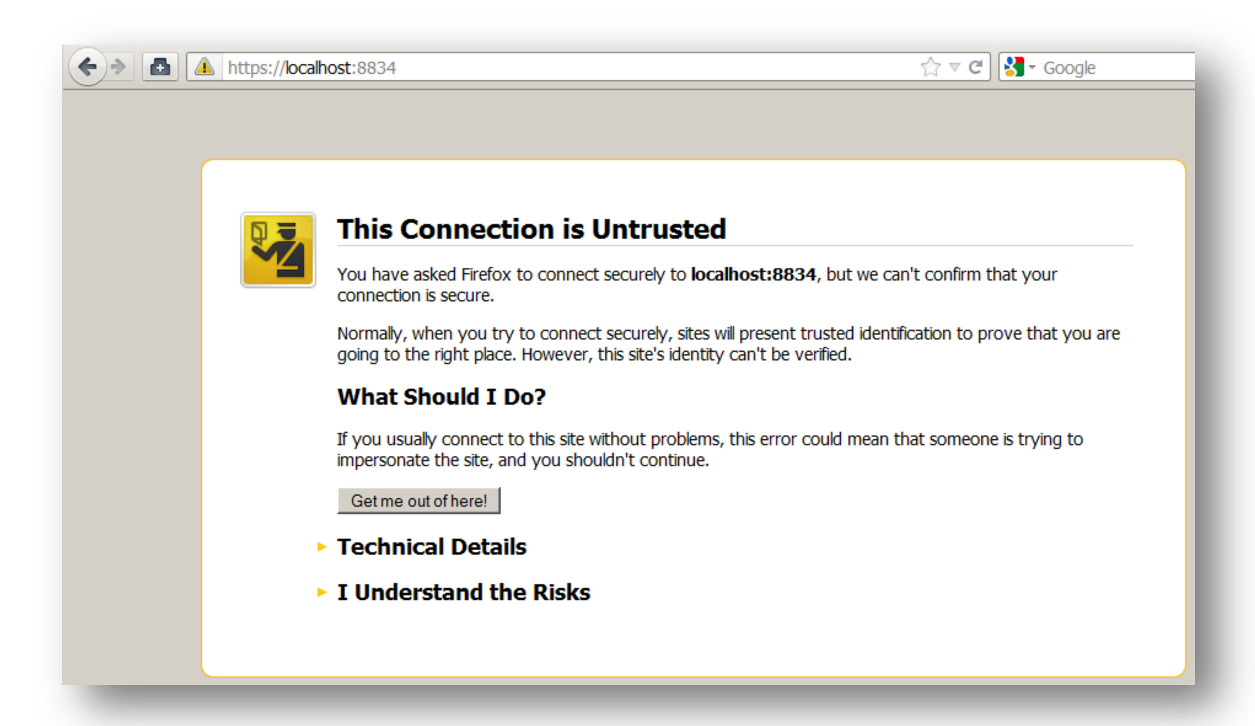
http://mybox:8834/) enthält. Ist der Hostname nicht im DNS vorhanden, dann müssen Sie die Verbindung zum Nessus-Server über eine IP-Adresse oder einen gültigen DNS-Namen herstellen.



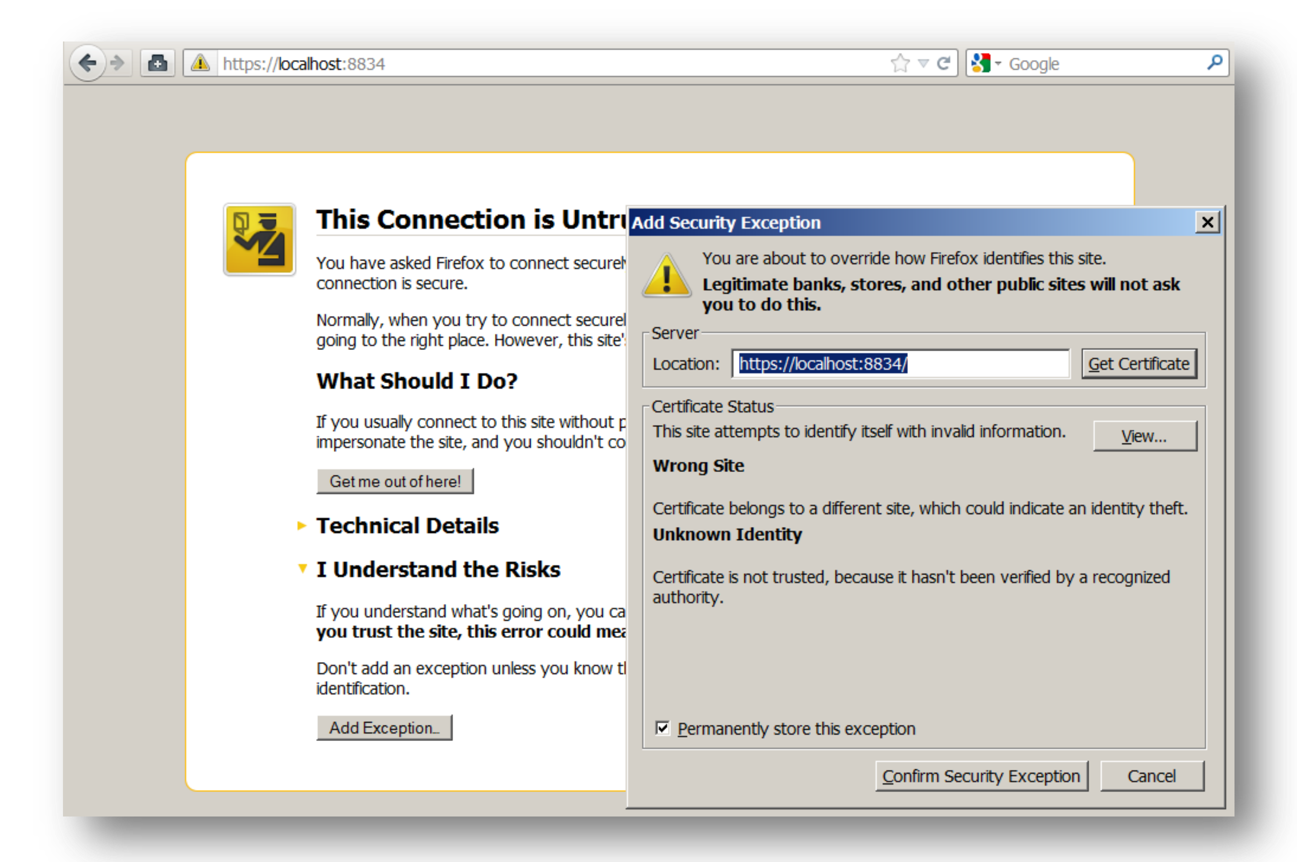
Auf dem Startbildschirm erscheint ein Warnhinweis, dass alle an die Nessus-Benutzeroberfläche gerichteten Daten SSL (HTTPS) verwenden. Wenn Sie zum ersten Mal eine Verbindung mit dem Nessus-Webserver herstellen, zeigt Ihr Browser eine Fehlermeldung an, laut der die Website nicht vertrauenswürdig ist, weil das SSL-Zertifikat selbstsigniert ist. Akzeptieren Sie das Zertifikat bei der erstmaligen Verbindung, um mit der Konfiguration fortzufahren. Hinweise zur Installation eines benutzerdefinierten Zertifikats werden im weiteren Verlauf dieses Dokuments im Abschnitt „Nessus mit angepasstem SSL-Zertifikat konfigurieren“ behandelt.



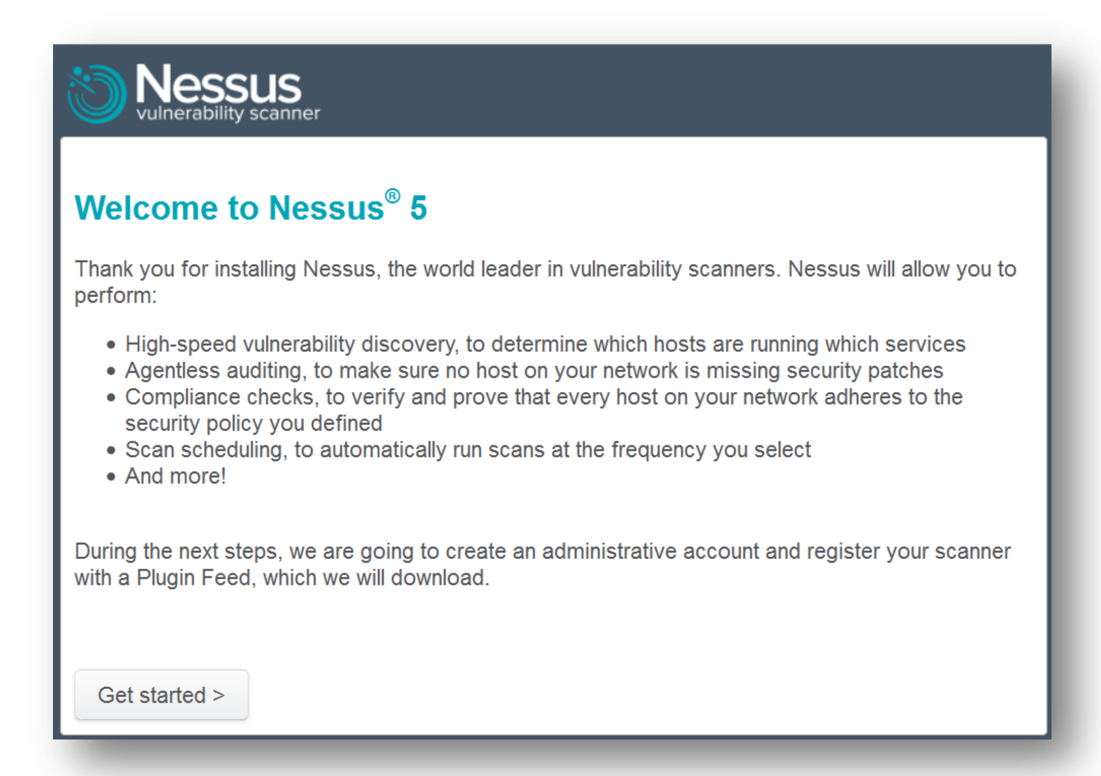
Aufgrund der technischen Implementierung von SSL-Zertifikaten ist es nicht möglich, mit Nessus ein Zertifikat auszuliefern, das für Browser vertrauenswürdig wäre. Sie können ein angepasstes, für Ihre Organisation ausgestelltes SSL-Zertifikat verwenden, um den Warnhinweis zukünftig zu vermeiden.



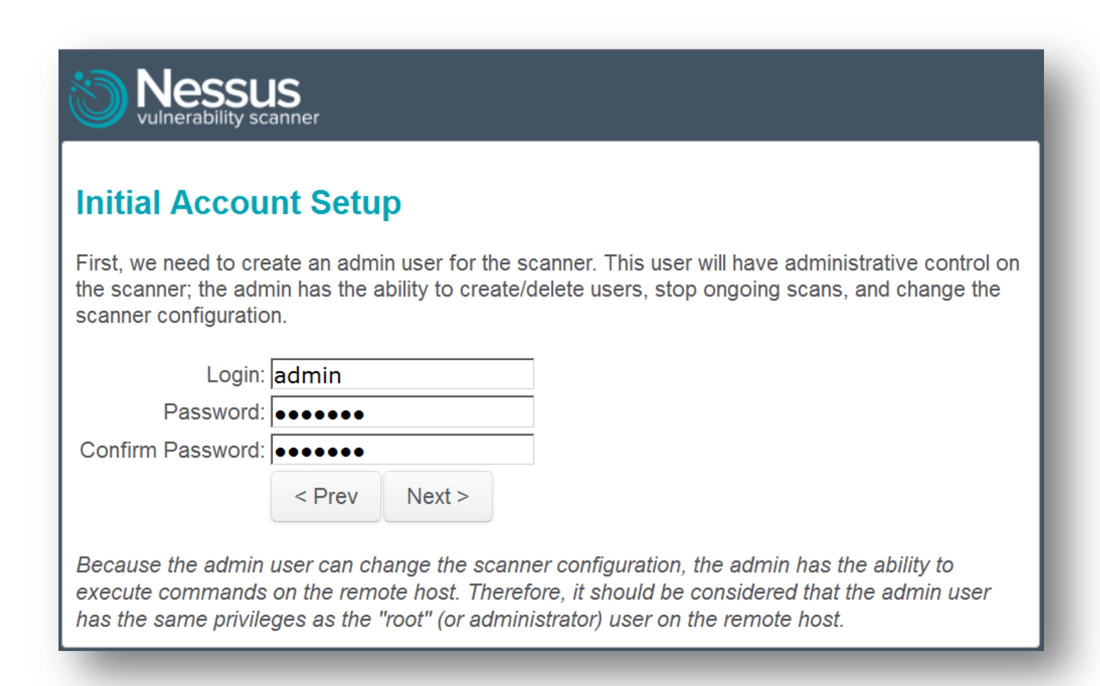
Abhängig vom verwendeten Browser wird unter Umständen ein weiteres Dialogfeld angezeigt, in dem Sie das Zertifikat annehmen können:



Nach dem Annehmen des Zertifikats werden Sie zum ersten Registrierungsbildschirm weitergeleitet, mit dem der eigentliche Vorgang beginnt:



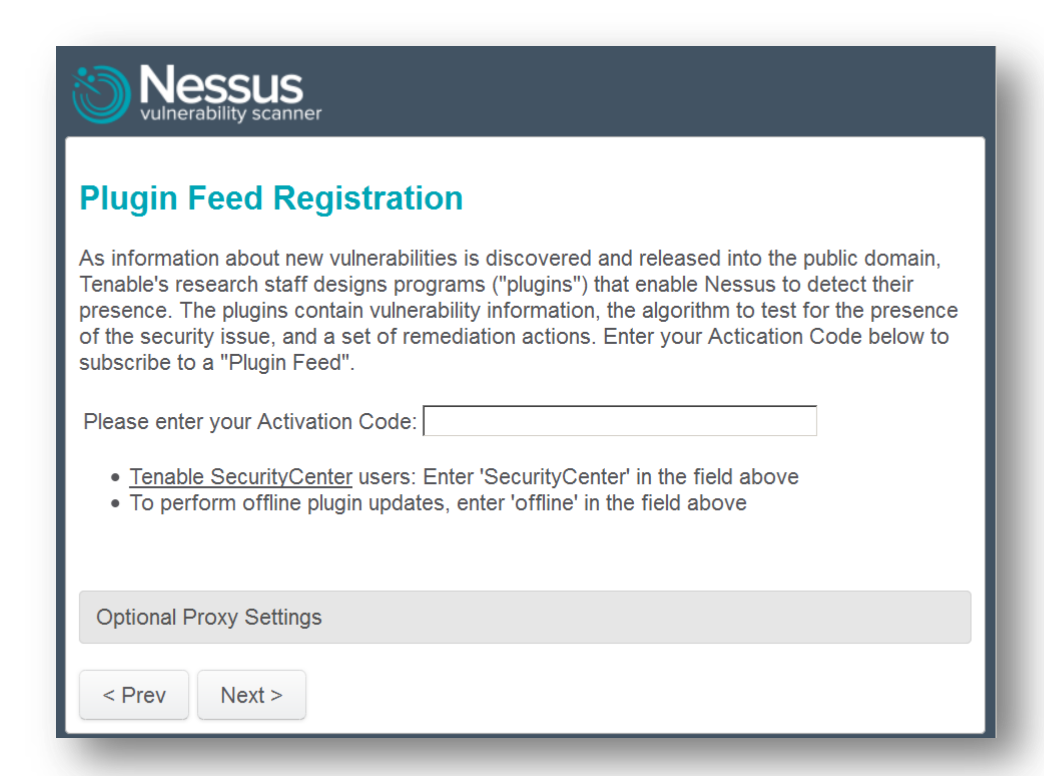
Der erste Schritt besteht darin, ein Konto für den Nessus-Server zu erstellen. Es handelt sich bei diesem Konto um ein Administratorkonto mit Zugriff auf Befehle des Betriebssystems, unter dem Nessus installiert wurde, weswegen Sie dieses Konto mit der gleichen Sorgfalt behandeln sollten wie jedes andere Administratorkonto:



Auf dem nächsten Bildschirm wird ein Plugin-Aktivierungscode abgefragt. Außerdem können Sie hier optionale Proxyeinstellungen konfigurieren. Wenn Sie nicht über einen Code verfügen, können Sie diesen auf dem Tenable Support Portal oder bei einem Vertriebspartner anfordern. Nach der Registrierung erhalten Sie eine E-Mail mit einem Link zur Aktivierung des Codes. Sie müssen den Code innerhalb von 24 Stunden aktivieren, damit Nessus einsatzbereit bleibt.



Wenn Sie Tenable SecurityCenter verwenden, werden der Aktivierungscode und Plugin-Updates über SecurityCenter verwaltet. Zur Kommunikation mit SecurityCenter muss Nessus gestartet werden, was gewöhnlich ohne einen gültigen Aktivierungscode und Plugins nicht möglich ist. Damit diese Anforderung von Nessus ignoriert wird und ein Start erfolgen kann (und die Informationen so aus SecurityCenter abgerufen werden können), geben Sie „SecurityCenter“ (in der angegebenen Schreibweise und ohne Anführungszeichen) in das Feld „Activation Code“ („Aktivierungscode“) ein. Nach dem Start von Nessus ist die Erstinstallation und -konfiguration des Nessus-Scanners für SecurityCenter-Benutzer abgeschlossen. Diese können nun mit dem Abschnitt „Mit SecurityCenter arbeiten“ fortfahren.





Wenn Sie Ihre Nessus-Kopie nicht registrieren, können Sie weder neue Plugins beziehen noch den Nessus-Server starten. Hinweis: Beim Aktivierungscode wird die Groß-/Kleinschreibung nicht unterschieden.

Wenn sich Ihr Nessus-Server in einem Netzwerk befindet, das über einen Proxy mit dem Internet kommuniziert, klicken Sie auf „**Optional Proxy Settings**“ („Optionale Proxyeinstellungen“), um die erforderlichen Informationen einzugeben. Die Proxyeinstellungen können jederzeit nach Abschluss der Installation eingegeben werden.

Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. Enter your Actication Code below to subscribe to a "Plugin Feed".

Please enter your Activation Code:

- Tenable SecurityCenter users: Enter 'SecurityCenter' in the field above
- To perform offline plugin updates, enter 'offline' in the field above

Optional Proxy Settings

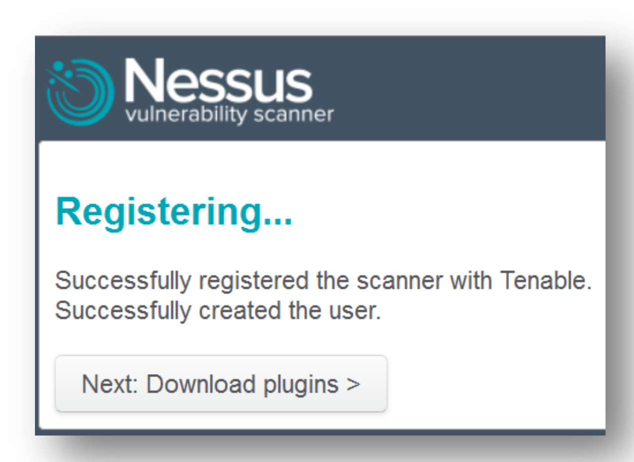
Proxy hostname:
Proxy username:
Proxy password:
Proxy password (again):

< Prev   Next >

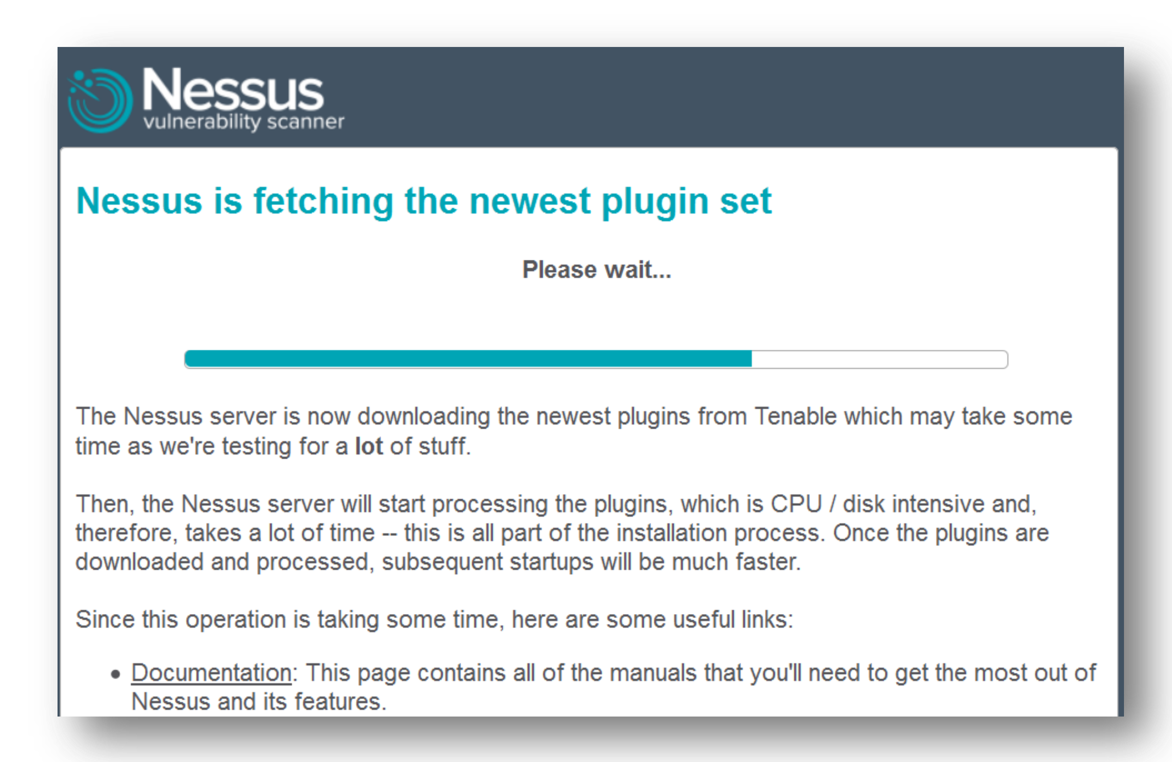


Wenn Sie bei der Aktivierung „offline“ wählen, beachten Sie, dass bei „offline“ die Groß-/Kleinschreibung beachtet wird.

Im nächsten Schritt muss der Aktivierungscode eingegeben werden, den Sie bereits über die Registrierungsseite von Tenable Nessus erhalten haben. Klicken Sie nach erfolgreicher Eingabe des Aktivierungscodes und der **optionalen** Konfiguration der Proxyeinstellungen auf „**Next**“ („Weiter“), um Ihren Scanner zu registrieren:



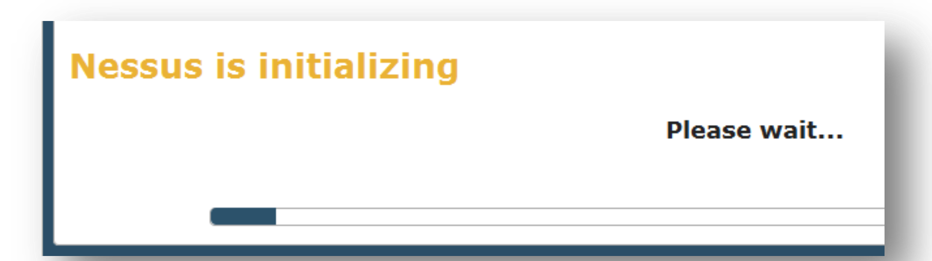
Nach der Registrierung müssen die Plugins durch Nessus von Tenable heruntergeladen werden. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen, da eine beträchtliche Menge Daten heruntergeladen, die Dateiintegrität überprüft und aus diesen Daten dann eine interne Datenbank kompiliert wird:





Nach der erstmaligen Registrierung lädt Nessus die Plugins über Port 443 von plugins.nessus.org, plugins-customers.nessus.org oder plugins-us.nessus.org im Hintergrund herunter.

Nach Download und Kompilierung der Plugins wird die Nessus-Benutzeroberfläche initialisiert, und der Nessus-Server wird gestartet:

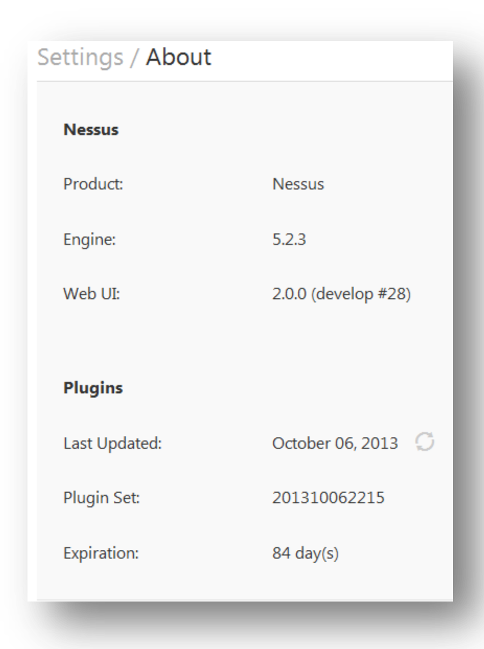


Nach der Initialisierung ist Nessus einsatzbereit.



Melden Sie sich unter Verwendung der bei der Installation erstellten Administratoranmeldedaten bei der Nessus-Benutzeroberfläche an, um den Zugriff zu überprüfen.

Klicken Sie nach der Authentifizierung auf den Abwärtspfeil neben dem Benutzernamen (z. B. „admin") und wählen Sie „**Settings**" („Einstellungen") aus, um die Informationen zu Nessus und zum aktuellen Feed anzuzeigen.

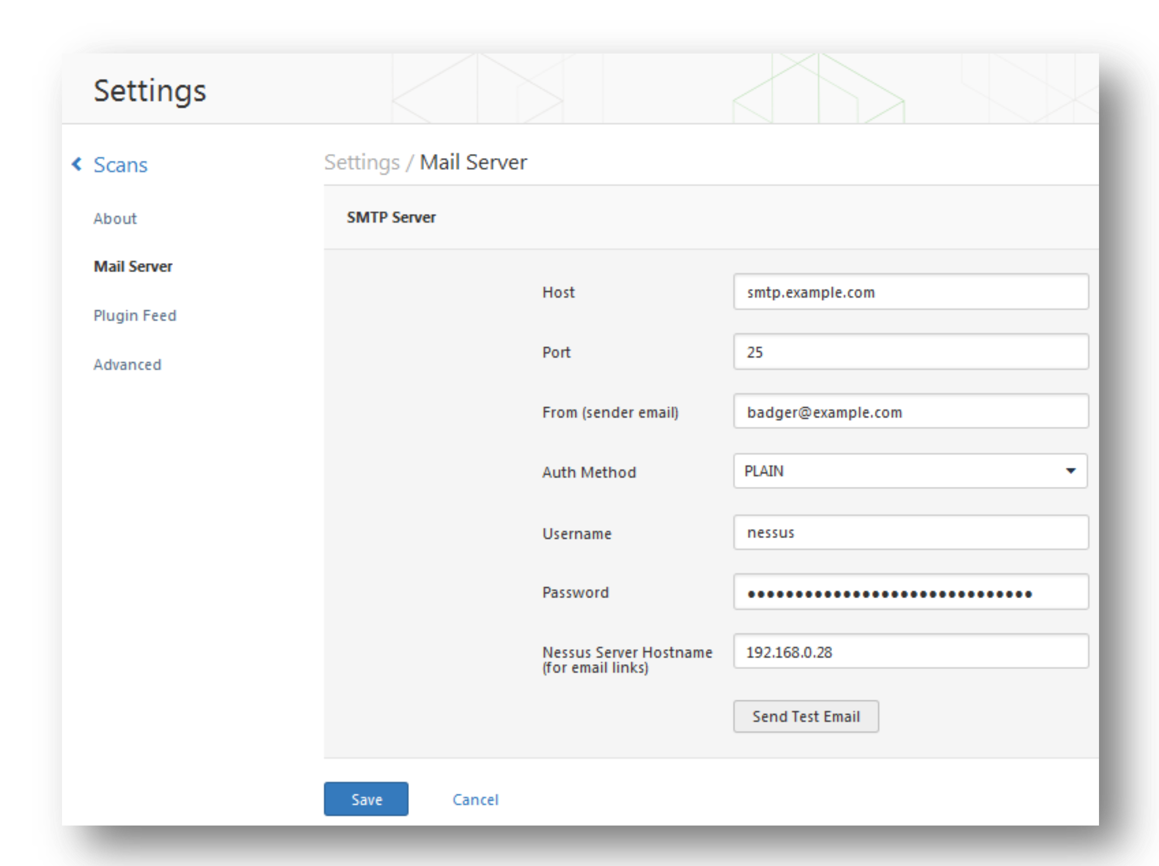


Konfiguration

Beginnend mit Nessus 5 wird die gesamte Nessus-Serverkonfiguration über die Benutzeroberfläche verwaltet. Die Datei **`nessusd.conf`** wird nicht mehr verwendet. Außerdem werden Proxyeinstellungen, die Registrierung von Feed-Abonnements und Offlineupdates über die Oberfläche verwaltet.

Mailserver

Die Registerkarte „**Mail Server**“ im Menü „**Settings**“ („Einstellungen“), das Sie über das Dropdownfeld oben links auf dem Bildschirm aufrufen, ermöglicht die Konfiguration eines SMTP-Servers, damit die Ergebnisse abgeschlossener Scans automatisch per E-Mail versandt werden.

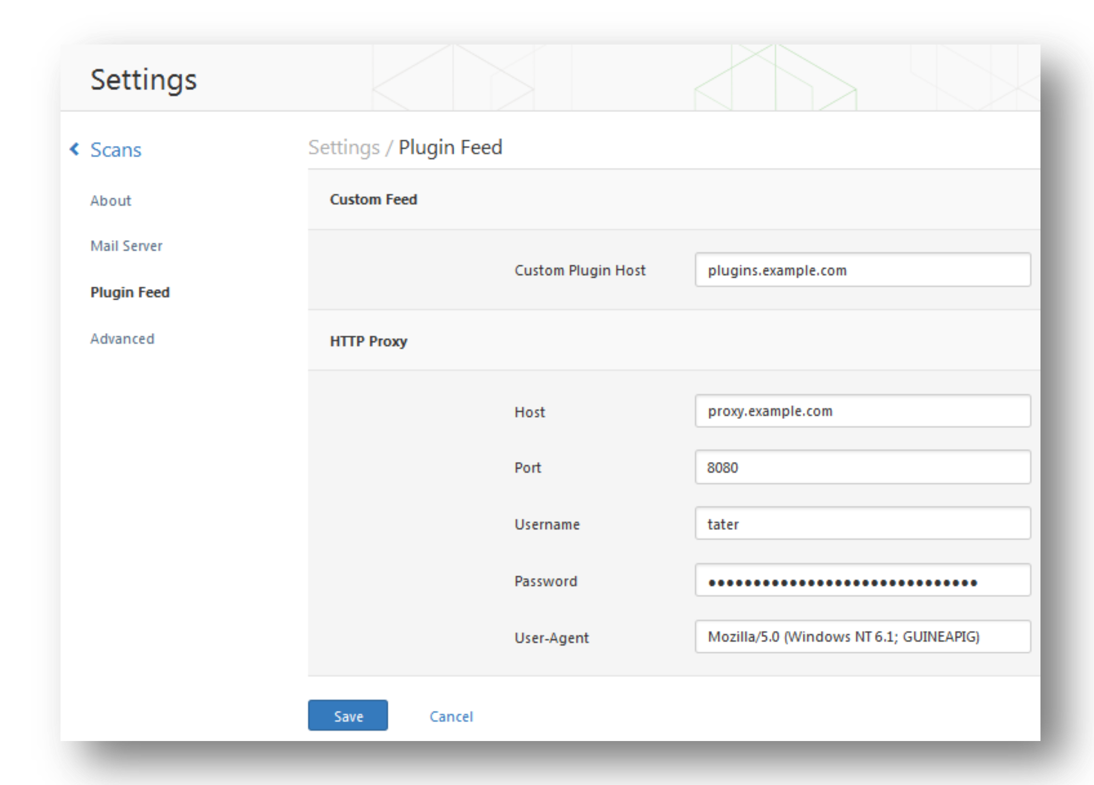


Option	Beschreibung
Host	Host oder IP-Adresse des SMTP-Servers (z. B. „smtp.example.com“)
Port	Port des SMTP-Servers (z. B. 25)
From (sender email) (Absenderadresse der E-Mail)	Absenderadresse der Berichts-E-Mail
Auth Method (Authentifizierungsmethode)	Authentifizierungsmethode auf dem SMTP-Server. Unterstützt werden „None“, „Plain“, „NTLM“, „Login“ und „CRAM-MD5“.
Username (Benutzername)	Benutzername zur Authentifizierung auf dem SMTP-Server
Password (Kennwort)	Kennwort zum Benutzernamen
Nessus Server Hostname (for email links) (Hostname	IP-Adresse oder Hostname des Nessus-Servers. Beachten Sie, dass diese Vorgehensweise nur funktioniert, wenn der Nessus-Host von dem Benutzer, der den

des Nessus-Servers – für E-Mail-Verbindungen)	Bericht lesen soll, erreicht werden kann.

Einstellungen für den Plugin-Feed

Die Registerkarte „**Plugin Feed**" im Menü „**Settings**", das Sie über das Dropdownfeld oben links auf dem Bildschirm aufrufen, ermöglicht die Konfiguration des Webproxys für Plugin-Updates. Diese ist erforderlich, wenn der gesamte Webdatenverkehr in Ihrem Unternehmen über einen Firmenproxy geführt wird:



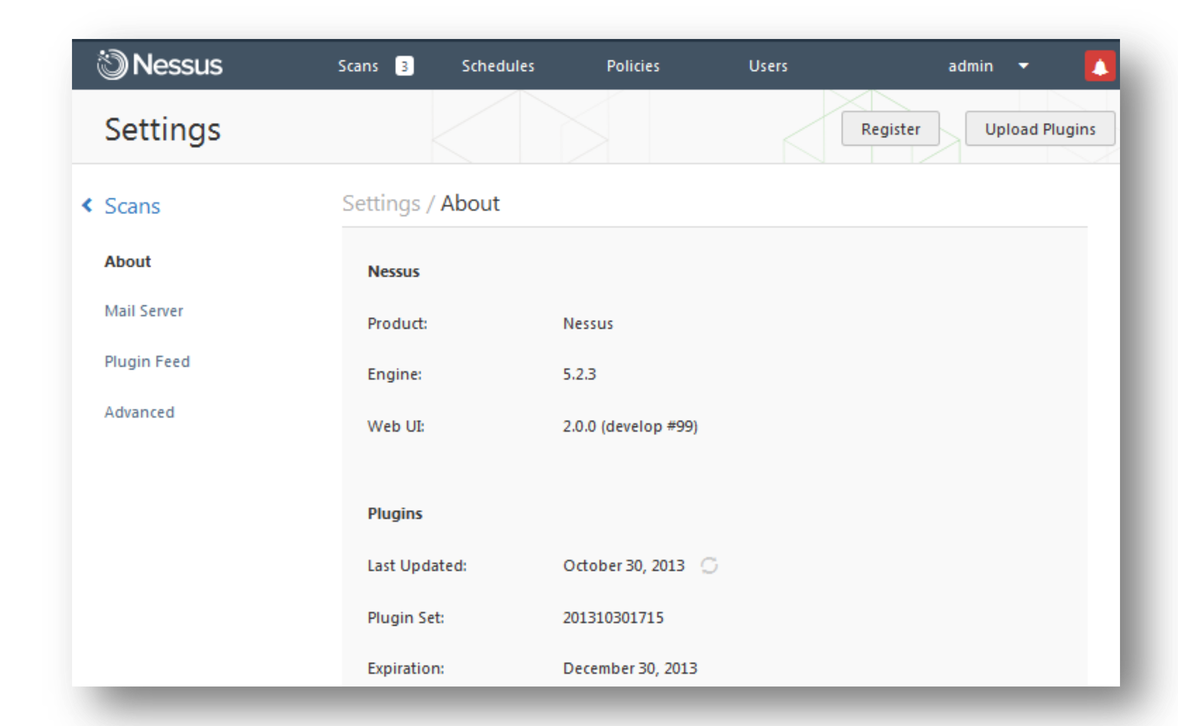
Zur Steuerung der Proxyeinstellungen sind sechs Felder vorhanden, von denen jedoch nur die Angaben für Host und Port obligatorisch sind. Den Benutzernamen und ein Kennwort können Sie ggf. optional eingeben.

Option	Beschreibung
Custom Plugin Host (Benutzerdefinierter Plugin-Host)	Optional: Hiermit können Sie die Aktualisierung von Plugins über einen bestimmten Host festlegen. Müssen die Plugins beispielsweise über eine Website aktualisiert werden, die in den USA ansässig ist, dann geben Sie hier „plugins-us.nessus.org" an.
Host	Host oder IP-Adresse des Proxys (z. B. „proxy.example.com")
Port	Port des Proxys (z. B. „8080")
Username (Benutzername)	Optional: Erlaubt die Angabe eines für die Proxynutzung ggf. erforderlichen Benutzernamens (z. B. „MMuster")
Password (Kennwort)	Optional: Erlaubt die Angabe eines für die Proxynutzung ggf. erforderlichen Kennworts (z. B. „m33rschw31nchen")

User-Agent (Benutzer-Agent)	Optional: Falls der verwendete Proxy bestimmte HTTP-User-Agents ausfiltert, kann hier eine benutzerdefinierte User-Agent-Zeichenfolge angegeben werden.

Aktivierungscodes zurücksetzen und Offline-Updates ausführen

Nach der erstmaligen Eingabe des Aktivierungscodes während des Setupvorgangs werden Änderungen des Codes über die Registerkarte „**About**“ („Info“) unter „**Settings**“ („Einstellungen“) vorgenommen. Sie rufen diesen Bildschirm auf, indem Sie auf der Benutzeroberfläche oben rechts neben dem Benutzernamen auf den Abwärtspfeil klicken und „**Settings**“ auswählen. Auf diesem Bildschirm werden oben rechts Schaltflächen für „**Register**“ („Registrieren“) und „**Upload Plugins**“ („Plugins hochladen“) angezeigt. Durch Eingabe des neuen Codes in das Feld „**Update Registration**“ („Registrierung aktualisieren“) der Schaltfläche „**Register**“ und Anklicken von „**Save**“ („Speichern“) wird der Nessus-Scanner mit dem neuen Code aktualisiert. (Dies kann beispielsweise erforderlich sein, wenn Sie von Nessus Home auf eine kostenpflichtige Nessus-Version umsteigen).



Im Abschnitt „**Upload Plugins**“ („Plugins hochladen“) können Sie ein Plugin-Archiv zur Verarbeitung festlegen. Weitere Details zur Offline-Aktualisierung finden Sie im Abschnitt „Nessus ohne Internetzugang“ weiter unten in diesem Dokument.



Die herkömmliche Clientnutzung über das NTP-Protokoll wird in Nessus 5 unterstützt, steht jedoch nur Kunden kostenpflichtiger Nessus-Versionen zur Verfügung.



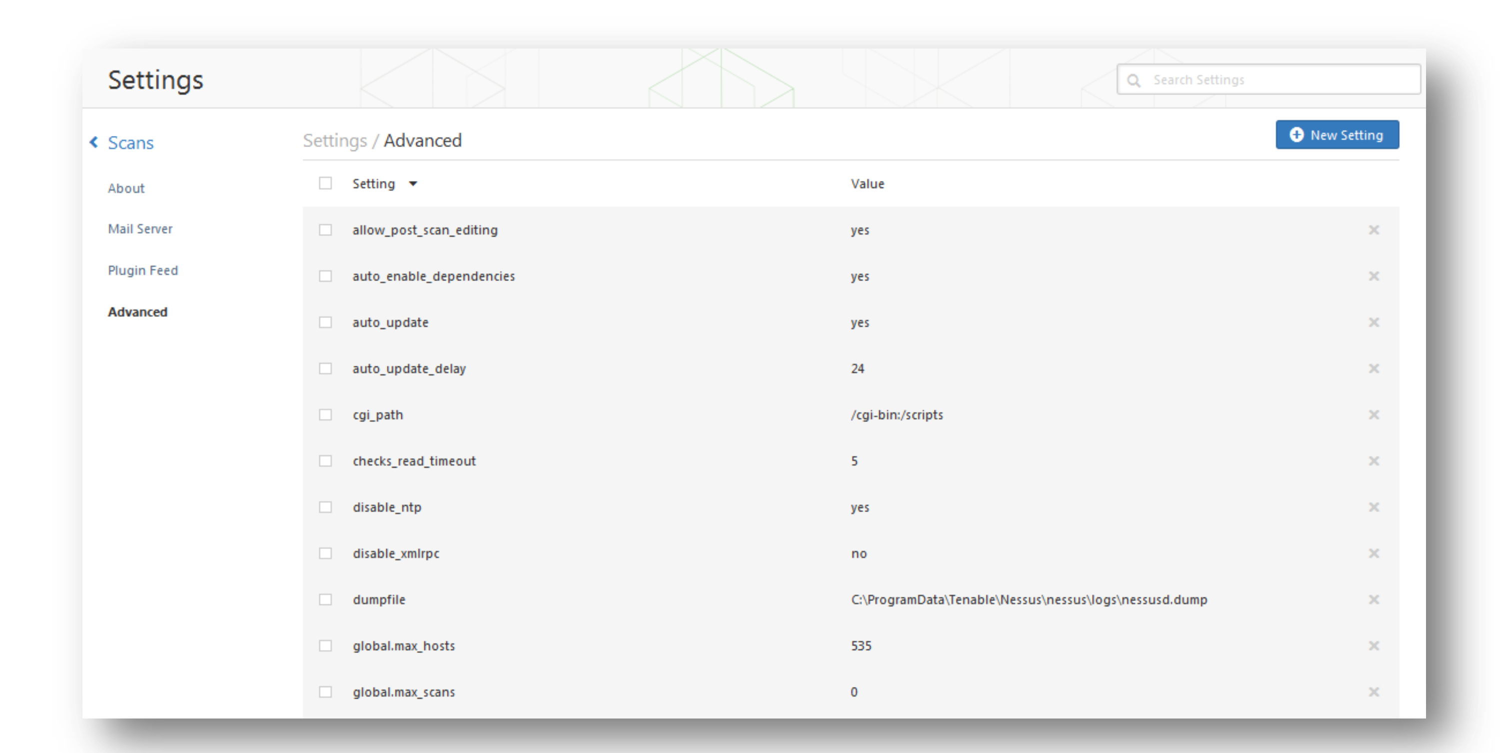
Wenn Sie den Registrierungscode für einen gegebenen Scanner überprüfen müssen, können Sie jederzeit die Option `--code-in-use` für das Programm `nessus-fetch` verwenden. Beachten Sie, dass Sie für diese Option Administratorrechte und eine Netzwerkverbindung brauchen.

Erweiterte Konfigurationsoptionen

Mithilfe einer Vielzahl von Konfigurationsoptionen ermöglicht Nessus eine sehr fein abgestufte Steuerung des Scannerbetriebs. Auf der Registerkarte „Advanced" („Erweitert"), erreichbar über das Dropdownmenü oben links, kann ein Administrator diese Einstellungen bearbeiten.



ACHTUNG: An der Nessus-Scannerkonfiguration vorgenommene Änderungen sind für ALLE Nessus-Benutzer gültig. Bearbeiten Sie diese Optionen nur mit größter Sorgfalt.



Diese Option lässt sich konfigurieren, indem das entsprechende Feld bearbeitet und dann auf die Schaltfläche „Save" („Speichern") unten auf dem Bildschirm geklickt wird. Außerdem kann die Option durch Anklicken der Schaltfläche ✖ vollständig entfernt werden.

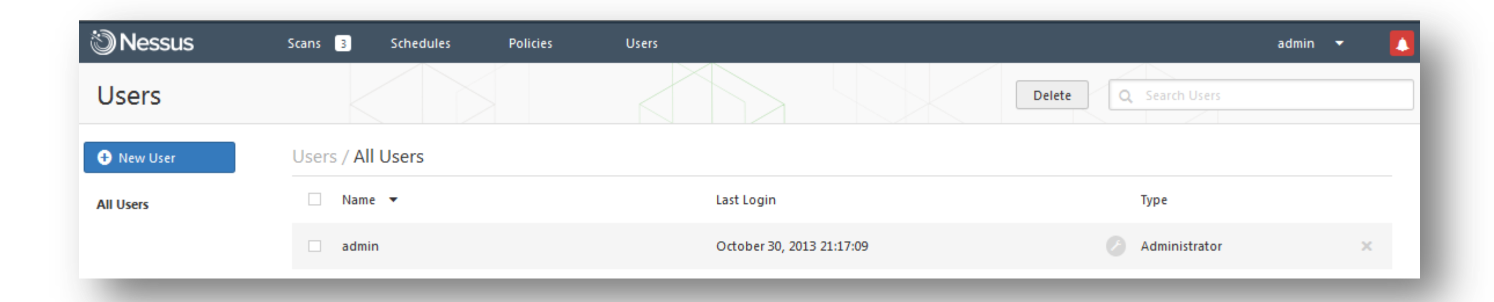
Standardmäßig kommuniziert die Nessus-Benutzeroberfläche über Port 8834. Setzen Sie `xmlrpc_listen_port` auf den gewünschten Port, um diese Einstellung zu ändern. Die Verarbeitung dieser Änderung durch den Nessus-Server kann einige Minuten in Anspruch nehmen.

Sollten weitere Einstellungen erforderlich sein, dann klicken Sie auf die Schaltfläche „**Add Preference Item**" („Einstellung hinzufügen"), geben den Namen und den Wert ein und klicken auf „**Save**". Nach dem Ändern und Speichern einer Einstellung kann die Verarbeitung dieser Änderung durch Nessus einige Minuten in Anspruch nehmen.

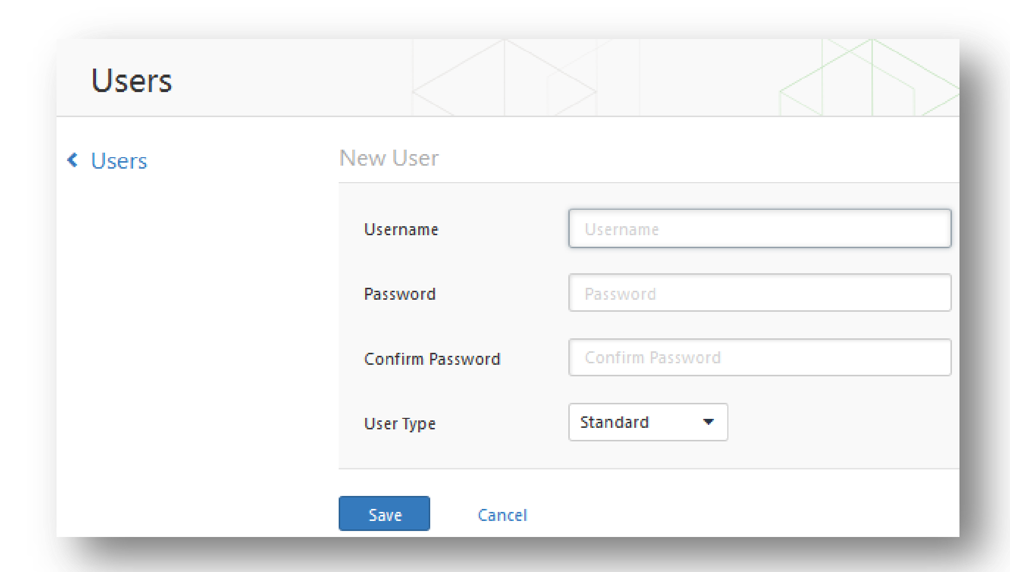
Ausführliche Informationen zu den einzelnen Konfigurationsoptionen finden Sie im Abschnitt „Nessus-Daemon konfigurieren (für fortgeschrittene Benutzer)" dieses Dokuments.

Nessus-Benutzer erstellen und verwalten

Bei der erstmaligen Einrichtung wird ein Administratorkonto erstellt. Melden Sie sich mit den Anmeldedaten, die während der Einrichtung angegeben wurden, bei der Nessus-Benutzeroberfläche an. Klicken Sie nach erfolgreicher Authentifizierung oben im Fenster auf „**Users**" („Benutzer"):

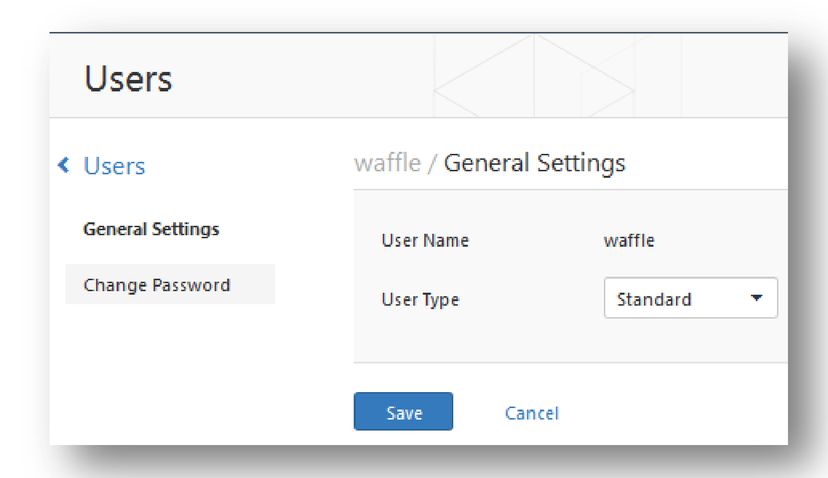


Klicken Sie zur Erstellung eines neuen Benutzers oben links auf „**New User**" („Neuer Benutzer"). Nun wird ein Dialogfeld geöffnet, in dem die erforderlichen Informationen abgefragt werden:



Geben Sie den Benutzernamen und das Kennwort ein, bestätigen Sie das Kennwort und legen Sie fest, ob der Benutzer Administratorrechte erhalten soll.

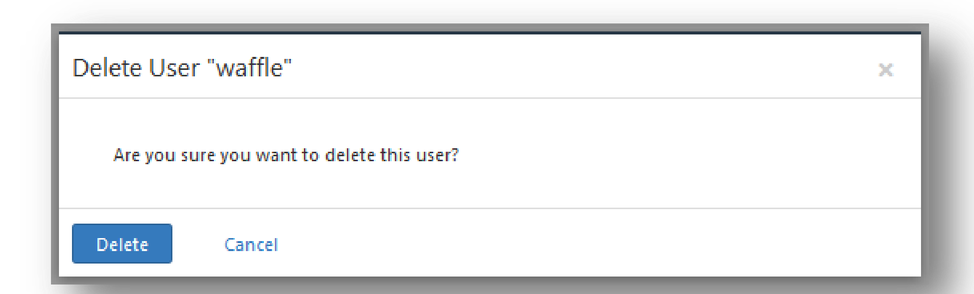
Wenn ein Benutzerkonto geändert werden muss, klicken Sie auf den Benutzer:





Sie können einen Benutzer nicht umbenennen. Wenn Sie den Namen eines Benutzers ändern möchten, müssen Sie den Benutzer löschen und dann einen neuen Benutzer mit dem passenden Anmeldenamen erstellen.

Aktivieren Sie zum Entfernen eines Benutzers entweder das Kontrollkästchen rechts neben dem Kontonamen in der Liste und wählen Sie dann oben „**Delete**" („Löschen"), oder klicken Sie auf das „**X**" rechts neben dem betreffenden Kontonamen.





Ein Benutzer, der kein Administrator ist, kann weder Plugins in Nessus hochladen noch einen Remoteneustart durchführen (was nach einem Plugin-Upload erforderlich ist) oder die Konfigurationseinstellungen **`max_hosts`** und **`max_checks`** außer Kraft setzen. Wenn für den Benutzer eine Verwendung von SecurityCenter vorgesehen ist, muss es sich um einen Administrator handeln. SecurityCenter verwaltet eine eigene Benutzerliste und legt Berechtigungen für seine Benutzer fest.

Müssen Sie für ein Nessus-Benutzerkonto Beschränkungen konfigurieren, so tun Sie dies über die Befehlszeile. Weitere Informationen erhalten Sie im Abschnitt „Nessus über die Befehlszeile verwenden und verwalten" im weiteren Verlauf dieses Dokuments.

Nessus-Daemon konfigurieren (für fortgeschrittene Benutzer)

Das Konfigurationsmenü für die Nessus-Benutzeroberfläche enthält verschiedene konfigurierbare Optionen. Hier legen Sie beispielsweise die maximale Anzahl von Tests und gleichzeitig zu scannenden Hosts, die von **`nessusd`** zu verwendenden Ressourcen, die Geschwindigkeit, mit der Daten gelesen werden sollen, und viele andere Optionen fest.

Es wird empfohlen, diese Einstellungen zu überprüfen und an die zu scannende Umgebung anzupassen. Die vollständige Liste der Konfigurationsoptionen wird am Ende dieses Abschnitts erläutert.

Insbesondere die Parameter **max_hosts** und **max_checks** können erhebliche Auswirkungen auf die Fähigkeit Ihres Nessus-Systems zur Durchführung von Scans sowie auf jene Systeme in Ihrem Netzwerk haben, die auf Sicherheitslücken gescannt werden. Gehen Sie deshalb bei der Konfiguration dieser beiden Werte mit Sorgfalt vor.

Für die beiden Parameter sind die folgenden Standardwerte festgelegt, die auch im Konfigurationsmenü erscheinen:

Option	Wert
max_hosts	40
max_checks	5

Beachten Sie, dass diese Einstellungen auf der Ebene des einzelnen Scanvorgangs außer Kraft gesetzt werden, wenn Tenable SecurityCenter oder eine entsprechend angepasste Richtlinie auf der Nessus-Benutzeroberfläche verwendet werden. Bearbeiten Sie zur Ansicht oder Änderung dieser Optionen für eine bestimmte Scanvorlage in SecurityCenter die „**Scan Options**“ („Scanoptionen“) der Vorlage. Bearbeiten Sie auf der Nessus-Benutzeroberfläche die Scanrichtlinie und klicken Sie dann auf die Registerkarte „Options“ („Optionen“).



Beachten Sie, dass der **max_checks** Parameter einen fest eingestellten Maximalwert von 15 hat. Werte, die größer als 5 sind, führen häufig zu unerwünschten Auswirkungen, da die meisten Server eine größere Zahl aggressiver Anfragen nicht gleichzeitig bearbeiten können.

Hinweise zu „max_hosts“:

Wie der Name bereits andeutet, ist dies die maximale Anzahl von Zielsystemen, die gleichzeitig gescannt werden können. Je höher die Zahl gleichzeitig durch einen einzelnen Nessus-Scanner gescannter Systeme, desto schwerwiegender sind die Auswirkungen auf RAM, Prozessor und Netzwerkbandbreite des Scannersystems. Beachten Sie, wenn Sie den Wert für **max_hosts** festlegen, die Hardwarekonfiguration des Scannersystems und die anderen Anwendungen, die darauf ausgeführt werden.

Da auch eine Anzahl anderer Faktoren, die für Ihre Scanumgebung charakteristisch sind (z. B. die Richtlinien Ihrer Organisation in Bezug auf Scans, der sonstige Datenverkehr im Netzwerk oder die Wirkung eines bestimmten Scantyps auf Ihre gescannten Hosts), sich auf Ihre Nessus-Scans auswirken werden, werden Sie experimentieren müssen, um die optimale Einstellung für **max_hosts** zu finden.

Ein eher konservativer Ausgangspunkt für die Ermittlung der besten **max_hosts**-Einstellung in einer Unternehmensumgebung ist der Wert „20“ auf einem UNIX-basierten Nessus-System und der Wert „10“ auf einem Nessus-Scanner unter Windows.

Neben **max_hosts** lässt der Server eine **global.max_hosts** Einstellung zu, die die Gesamtanzahl der Hosts steuert, die gleichzeitig von allen Benutzern gescannt werden können. Vor Nessus 5.2.0 traf die Beschränkung durch **max_hosts** nicht auf Administratoren zu – anders als die Einstellung **global.max_hosts**. Seit Nessus 5.2.0 gelten für Administratoren dieselben Beschränkungen durch beide Einstellungen. Hierdurch soll eine übermäßige Belastung des Scanservers vermieden werden, weil diese negative Auswirkungen auf andere Benutzer haben könnte.

Hinweise zu „max_checks“:

Dieser Parameter gibt die Anzahl gleichzeitiger Tests oder Plugins an, die während des Scannens eines einzelnen Zielhosts ausgeführt werden. Beachten Sie, dass, wenn Sie diesen Wert zu hoch wählen, die gescannten Systeme je nachdem, welche Plugins Sie beim Scan nutzen, überlastet werden können.

Multiplizieren Sie die Werte von **max_checks** und **max_hosts**, um die Anzahl gleichzeitiger Tests zu ermitteln, die zu einem beliebigen Zeitpunkt während des Scans möglicherweise ausgeführt werden. Weil **max_checks** und **max_hosts** sich gegenseitig beeinflussen, kann auch ein zu hoher Wert für **max_checks** einen Ressourcenmangel auf einem Nessus-Scannersystem verursachen. Wie bei **max_hosts** müssen Sie auch bei **max_checks** experimentieren, um die optimale Einstellung zu finden. Im Zweifelsfall sollten Sie immer einen relativ niedrigen Wert auswählen.

Konfigurationsoptionen

Die folgende Tabelle enthält kurze Erläuterungen zu allen Optionen im Konfigurationsmenü. Viele dieser Optionen können über die Benutzeroberfläche konfiguriert werden, wenn eine Scanrichtlinie erstellt wird.

Option	Beschreibung
auto_enable_dependencies	Hiermit werden automatisch alle Plugins aktiviert, von denen andere Plugins abhängen. Wenn diese Option deaktiviert ist, werden unter Umständen auch dann nicht alle Plugins ausgeführt, wenn sie in einer Scanrichtlinie ausgewählt wurden.
auto_update	Automatische Plugin-Updates. Falls die Option aktiviert und Nessus registriert ist, werden die aktuellen Plugins automatisch von plugins.nessus.org abgerufen. Deaktivieren Sie die Option, wenn der Scanner sich in einem isolierten Netzwerk befindet, das keine Verbindung zum Internet hat.
auto_update_delay	Wartezeit zwischen zwei Updates in Stunden. Der zulässige Mindestwert beträgt vier (4) Stunden.
cgi_path	Gibt eine Liste von durch Doppelpunkte getrennten CGI-Pfaden an, die beim Testen von Webservern verwendet wird.
checks_read_timeout	Gibt den Lesetimeout für die Testsockets an.
disable_ntp	Deaktiviert das veraltete NTP-Protokoll.
disable_xmlrpc	Deaktiviert die neue XMLRPC-Schnittstelle (Webserverschnittstelle).
dumpfile	Gibt den Speicherort einer Speicherauszugsdatei zum Debuggen der Ausgabe an (sofern generiert).
enable_listen_ipv4	Hiermit wird Nessus angewiesen, auf IPv4 zu horchen.
enable_listen_ipv6	Hiermit wird Nessus angewiesen, auf IPv6 zu horchen, sofern das System die IPv6-Adressierung unterstützt.
global.max_scans	Werte ungleich null geben hier die maximale Anzahl Scans an, die parallel stattfinden dürfen. **Hinweis**: Wenn diese Option nicht verwendet wird, gibt es keine Begrenzung.
global.max_simult_tcp_ sessions	Maximale Anzahl gleichzeitiger TCP-Sitzungen zwischen allen Scans. **Hinweis**: Wenn diese Option nicht verwendet wird, gibt es keine Begrenzung.
global.max_web_users	Werte ungleich null geben hier die maximale Anzahl (Web-) Benutzer an, die parallel eine Verbindung herstellen dürfen. **Hinweis**: Wenn diese Option nicht verwendet wird, gibt es keine Begrenzung.
host.max_simult_tcp_ sessions	Maximale Anzahl gleichzeitiger TCP-Sitzungen je gescanntem Host.

listen_address	IPv4-Adresse, auf der auf eingehende Verbindungen gehorcht wird. Falls hier die Adresse 127.0.0.1 festgelegt ist, wird der Zugriff auf lokale Verbindungen beschränkt.
listen_port	Port, auf dem gehorcht wird (wird vom veralteten NTP-Protokoll verwendet). Wird für Verbindungen mit NessusClients vor Version 4.2 benötigt.
log_whole_attack	Gibt an, ob jedes Detail eines Angriffs protokolliert werden soll. Dies kann zum Debuggen nützlich sein, erfordert aber sehr viel Festplattenspeicher.
logfile	Gibt an, wo die Nessus-Logdatei gespeichert ist.
login_banner	Ein Textbanner, das vor der erstmaligen Anmeldung beim Flash- oder HTML5-Client angezeigt wird.
max_hosts	Maximale Anzahl während eines Scans gleichzeitig überprüfter Hosts.
max_checks	Maximale Anzahl gleichzeitiger Überprüfungen je getestetem Host.
max_simult_tcp_sessions	Maximale Anzahl gleichzeitiger TCP-Sitzungen je Scan.
nasl_log_type	Leitet den Ausgabetyp der NASL-Engine in `nessusd.dump` um.
nasl_no_signature_check	Bestimmt, ob Nessus alle NASL-Skripts als signiert betrachten soll. Die Auswahl „yes“ („ja“) ist unsicher und wird nicht empfohlen.
nessus_syn_scanner. global_throughput.max	Legt die maximale Anzahl der SYN-Pakete fest, die von Nessus während eines Portscans pro Sekunde versendet werden. Wie viele Hosts dabei parallel gescannt werden, spielt keine Rolle. Geben Sie je nach Empfindlichkeit des Remotegeräts möglichst hohe Werte für die SYN-Pakete an.
non_simult_ports	Gibt Ports an, die nicht gleichzeitig von zwei unterschiedlichen Plugins getestet werden sollten.
optimize_test	Hierdurch wird der Testvorgang optimiert. Wenn Sie hier den Wert „no“ („nein“) eintragen, benötigen Scans mehr Zeit, und in der Regel werden auch mehr Fehlalarme produziert.
paused_scan_timeout	Beendet einen unterbrochenen Scan zwangsweise nach der angegebenen Anzahl Minuten. Bei „0“ erfolgt kein Timeout.
plugin_upload	Gibt an, ob Administratoren Plugins hochladen können.
plugin_upload_suffixes	Suffixe von Plugins, die ein Administrator hochladen kann.
plugins_timeout	Gibt die maximale Aktivitätsdauer eines Plugins (in Sekunden) an.
port_range	Gibt den zu scannenden Portbereich an. Hier können die Schlüsselwörter „default“ („Standard“) oder „all“ („alle“) sowie eine kommagetrennte Liste mit Ports oder Portbereichen angegeben werden.
purge_plugin_db	Bestimmt, ob Nessus die Plugin-Datenbank bei jedem Update bereinigen soll. Hiermit wird festgelegt, dass die Plugin-Datenbank bei jedem Update entfernt, neu heruntergeladen und neu erstellt wird. Wenn Sie „yes“ („Ja“) auswählen, dauern alle Updates wesentlich länger.

qdb_mem_usage	Hiermit wird Nessus angewiesen, im Leerlauf mehr oder weniger Speicher zu verwenden. Wenn Nessus auf einem dedizierten Server ausgeführt wird, können Sie hier „high“ festlegen, um mehr Speicher zuzuweisen und die Leistungsfähigkeit so zu erhöhen. Wird Nessus hingegen auf einem Computer ausgeführt, der auch noch andere Aufgaben erledigt, dann wählen Sie hier „low“, um den Speicherbedarf erheblich zu beschränken. Diese Einstellung wirkt sich geringfügig auf die Leistung aus.
reduce_connections_on_ congestion	Verringert die Anzahl der parallel ausgeführten TCP-Sitzungen, wenn im Netzwerk Überlastungen erkannt wurden.
report_crashes	Hiermit werden anonym Berichte zu Abstürzen an Tenable übermittelt.
rules	Gibt an, wo die Regeldatei `nessusd.rules` von Nessus gespeichert ist. Die Datei **`nessusd.rules`** gilt auch für Nessus-Administratoren.
safe_checks	Sichere Tests nutzen die Bannererfassung, statt aktiv auf Sicherheitslücken zu testen.
save_knowledge_base	Speichert die Knowledge-Base zur späteren Benutzung auf der Festplatte.
silent_dependencies	Falls diese Option aktiviert ist, werden die Liste der Plugin-Abhängigkeiten und ihre Ausgaben nicht in den Bericht eingeschlossen. Ein Plugin kann als Bestandteil einer Richtlinie ausgewählt werden, die von der Ausführung anderer Plugins abhängt. Standardmäßig werden solche Plugin-Abhängigkeiten von Nessus ausgeführt, aber ihre Ausgabe wird nicht im Bericht aufgeführt. Wenn Sie diese Option auf „**no**“ festlegen, werden sowohl das ausgewählte Plugin als auch ggf. vorhandene Plugin-Abhängigkeiten im Bericht aufgeführt.
slice_network_addresses	Wenn diese Option festgelegt ist, scannt Nessus ein Netzwerk nicht inkrementell (d. h. in der Reihenfolge 10.0.0.1, 10.0.0.2, 10.0.0.3 usw.), sondern versucht, die Belastung gleichmäßig auf das Netzwerk zu verteilen. Die Reihenfolge kann dann beispielsweise 10.0.0.1, 10.0.0.127, 10.0.0.2, 10.0.0.128 usw. lauten.
source_ip	Im Falle eines Multihomed-Systems mit unterschiedlichen IP-Adressen im selben Subnetz wird dem Nessus-Scanner mithilfe dieser Option mitgeteilt, welche Netzwerkkarte bzw. IP-Adresse er für die Tests verwenden soll. Werden mehrere IP-Adressen angegeben, dann verwendet Nessus sie nacheinander immer dann, wenn eine Verbindung hergestellt wird.
ssl_cipher_list	Hiermit wird sichergestellt, dass nur sichere SSL-Verschlüsselungen beim Herstellen der Verbindung mit Port 1241 verwendet werden. Unterstützt werden das Schlüsselwort „strong“ oder allgemeine OpenSSL-Bezeichnungen, wie sie unter http://www.openssl.org/docs/apps/ciphers.html aufgeführt sind.
stop_scan_on_disconnect	Beendet das Scannen eines Hosts, dessen Verbindung während des Scans getrennt wurde.
stop_scan_on_hang	Beendet einen Scan, der offenbar stehengeblieben ist.
throttle_scan	Bei einer Prozessorüberlastung wird der Scanvorgang gedrosselt.
use_kernel_congestion_ detection	Hiermit werden die Scanaktivitäten erforderlichenfalls anhand vorliegender TCP-Netzüberlastungsmeldungen zurückgefahren.

www_logfile	Gibt an, wo die Logdatei des Nessus-Webservers (Benutzeroberfläche) gespeichert ist.
xmlrpc_idle_session_ timeout	XMLRPC-Sitzungstimeout bei Leerlauf (in Minuten)
xmlrpc_import_feed_ policies	Wenn hier die Einstellung „no“ gewählt wird, schließt Nessus die von Tenable bereitgestellten Standardscanrichtlinien nicht ein.
xmlrpc_listen_port	Port, auf dem der Nessus-Webserver horcht (wird vom neuen XMLRPC-Protokoll verwendet)
xmlrpc_min_password_len	Hiermit wird Nessus angewiesen, eine Richtlinie für die Länge eines Kennworts für Benutzer des Scanners zu erzwingen.

Standardmäßig ist **`report_crashes`** auf „yes“ festgelegt. Informationen, die sich auf einen Absturz in Nessus beziehen, werden an Tenable übermittelt und dort zur Beseitigung von Fehlern verwendet, um eine Software maximaler Qualität anbieten zu können. Personen- oder systembezogene Informationen werden nicht an Tenable übertragen. Personen- oder systembezogene Informationen werden nicht übertragen.



Zum Übernehmen bestimmter Einstellungen wie **`source_ip`** muss Nessus ggf. neu gestartet werden.

Nessus mit einem angepassten SSL-Zertifikat konfigurieren

Bei der Standardinstallation von Nessus wird ein selbstsigniertes SSL-Zertifikat verwendet. Wenn Sie zum ersten Mal die Weboberfläche für den Zugriff auf den Nessus-Scanner verwenden, zeigt Ihr Webbrowser eine Fehlermeldung an, laut der das Zertifikat nicht vertrauenswürdig ist:



Sie können ein angepasstes, für Ihre Organisation ausgestelltes SSL-Zertifikat verwenden, um zukünftige Warnungen im Browser zu vermeiden. Bei der Installation erstellt Nessus zwei Dateien, die das Zertifikat bilden: **`servercert.pem`** und **`serverkey.pem`**. Diese Dateien müssen durch Zertifikatsdateien ersetzt werden, die von Ihrer Organisation oder einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) generiert wurden.

Beenden Sie vor dem Ersetzen der Zertifikatsdateien den Nessus-Server. Ersetzen Sie die beiden Dateien, und starten Sie den Nessus-Server dann neu. Nachfolgend sollte bei Verbindungen mit dem Scanner keine Fehlermeldung mehr angezeigt werden, sofern das Zertifikat von einer vertrauenswürdigen CA stammt.

Die folgende Tabelle listet die Speicherorte der Zertifikatsdateien unter den einzelnen Betriebssystemen auf:

Betriebssystem	Speicherort für Zertifikatsdateien
Linux	**`/opt/nessus/com/nessus/CA/servercert.pem`** **`/opt/nessus/var/nessus/CA/serverkey.pem`**
FreeBSD	**`/usr/local/nessus/com/nessus/CA/servercert.pem`** **`/usr/local/nessus/var/nessus/CA/serverkey.pem`**
Windows Vista und neuer	**`C:\ProgramData\Tenable\Nessus\nessus\CA\`**
Windows XP/2003	**`C:\Dokumente und Einstellungen\All Users\Application Data\Tenable\Nessus\nessus\CA\`**
Mac OS X	**`/Library/Nessus/run/com/nessus/CA/servercert.pem`** **`/Library/Nessus/run/var/nessus/CA/serverkey.pem`**

Nessus 5 unterstützt SSL-Zertifikatsketten.



Sie können auch die Seite `https://[IP address]:8834/getcert` besuchen, um die Stamm-CA in Ihrem Browser zu installieren. Nachfolgend wird keine Warnung mehr angezeigt.

Zur Einrichtung einer Zwischenzertifikatskette muss eine Datei namens **`serverchain.pem`** im selben Verzeichnis abgelegt werden, in dem sich auch die Datei **`servercert.pem`** befindet. Sie sollte die 1-n Zwischenzertifikate (verkettete öffentliche Zertifikate) enthalten, die zur Bildung der vollständigen Zertifikatskette vom Nessus-Server bis zum eigentlichen Stammzertifikat (d. h. einem Zertifikat, das für den Browser des Benutzers vertrauenswürdig ist) verwendet werden.

Mit einem SSL-Zertifikat bei Nessus authentifizieren

SSL-Clientzertifikatsauthentifizierung

Nessus gestattet die Verwendung der SSL-Clientzertifikatsauthentifizierung. Auf diese Weise können SSL-Clientzertifikate, Smartcards oder die CAC-Authentifizierung verwendet werden, sofern der Browser für die jeweilige Methode konfiguriert ist.

Nessus unterstützt für Benutzerkonten eine Authentifizierung auf Kennwortbasis oder mithilfe eines SSL-Zertifikats. Zur Erstellung eines Benutzers für die SSL-Zertifikatsauthentifizierung wird das Utility **`nessus-mkcert-client`** auf der Befehlszeile des Nessus-Servers verwendet.

Nessus für Zertifikate konfigurieren

Der erste Schritt auf dem Weg zur Authentifizierung via SSL-Zertifikat besteht in der Konfiguration des Nessus-Webservers mit einem Serverzertifikat und einer Zertifizierungsstelle. Bei diesem Vorgang wird der Webserver so konfiguriert, dass er Zertifikaten, die von der Zertifizierungsstelle (Certificate Authority, CA) erstellt werden, zu Authentifizierungszwecken vertraut. Besitzer der im Zusammenhang mit Zertifikaten erstellten Dateien muss `root:root` sein. Die Standardberechtigungen sind angemessen.

1. Optional können Sie mit dem Befehl **nessus-mkcert** auf der Befehlszeile eine neue benutzerdefinierte Zertifizierungsstelle und ein Serverzertifikat für den Nessus-Server erstellen. Bei dieser Vorgehensweise werden die Zertifikate in den jeweils korrekten Verzeichnissen abgelegt.



> Wenn Sie zur Eingabe des Hostnamens aufgefordert werden, geben Sie den DNS-Namen oder die IP-Adresse des Servers im Browser ein (Beispiel: https://hostname:8834/ bzw. https://ipaddress:8834/). Das Standardzertifikat verwendet den Hostnamen.

2. Wenn anstelle des von Nessus generierten ein von einer Zertifizierungsstelle stammendes Zertifikat verwendet wird, erstellen Sie mithilfe des betreffenden Befehls für Ihr Betriebssystem eine Kopie des selbstsignierten Zertifikats der Zertifizierungsstelle:

   Linux/UNIX:
   ```
   # cp /opt/nessus/com/nessus/CA/cacert.pem /opt/nessus/com/nessus/CA/ORIGcacert.pem
   ```

   Windows Vista und neuer
   ```
   C:\> copy \ProgramData\Tenable\Nessus\nessus\CA\cacert.pem
   C:\ProgramData\Tenable\Nessus\nessus\CA\ORIGcacert.pem
   ```

   Windows XP und 2003:
   ```
   C:\> copy \Dokumente und Einstellungen\All Users\Application
   Data\Tenable\Nessus\nessus\CA\cacert.pem C:\Dokumente und Einstellungen\All
   Users\Application Data\Tenable\Nessus\nessus\CA\ORIGcacert.pem
   ```

3. Wenn die zur Authentifizierung verwendeten Zertifikate nicht vom Nessus-Server, sondern von einer anderen Zertifizierungsstelle erstellt werden, muss das CA-Zertifikat auf dem Nessus-Server installiert werden:

   Linux/UNIX:
   Kopieren Sie das CA-Zertifikat der Organisation nach **/opt/nessus/com/nessus/CA/cacert.pem**

   Windows Vista und neuer:
   Kopieren Sie das CA-Zertifikat der Organisation nach
   C:\ProgramData\Tenable\Nessus\nessus\CA\\cacert.pem

4. Windows XP und 2003:
   Kopieren Sie das CA-Zertifikat der Organisation nach: **C:\Dokumente und Einstellungen\All Users\Application Data\Tenable\Nessus\nessus\CA** Konfigurieren Sie den Nessus-Server auf die Zertifikatauthentifizierung. Nach Aktivierung der Zertifikatsauthentifizierung ist die Anmeldung mithilfe eines Benutzernamens und eines Kennworts deaktiviert.

   Linux/UNIX:
   ```
   # /opt/nessus/sbin/nessus-fix --set force_pubkey_auth=yes
   ```

   Windows:
   ```
   C:\> \Programme\Tenable\Nessus\nessus-fix --set force_pubkey_auth=yes
   ```

5. Wenn die Zertifizierungsstelle vorhanden und die Option **force_pubkey_auth** aktiviert ist, starten Sie die Nessus-Dienste mit dem Befehl **service nessusd restart** neu.

Wenn Sie die erforderlichen CA-Zertifikate in Nessus konfiguriert haben, können sich die Benutzer nachfolgend mithilfe von SSL-Clientzertifikaten, Smartcards oder CACs anmelden.

SSL-Zertifikate für die Anmeldung erstellen

Damit sich Benutzer mit SSL-Zertifikaten bei einem Nessus-Server anmelden können, müssen die Zertifikate mit dem passenden Utility erstellt werden. Hierbei kommt das Befehlszeilenprogramm **nessus-mkcert-client** zum Einsatz.

Es werden sechs Fragen gestellt, auf deren Basis dann die Vorgaben für die Erstellung von Benutzern in der aktuellen Sitzung festgelegt werden. Sie betreffen die Gültigkeitsdauer des Zertifikats, Land, Bundesstaat oder Region, Standort, Organisation und Organisationseinheit. Die Vorgaben für diese Optionen können während der eigentlichen Erstellung des Benutzers ggf. geändert werden. Die Benutzer werden dann nacheinander wie angefordert erstellt. Am Ende des Vorgangs werden die Zertifikate wie erforderlich kopiert und nachfolgend für die Anmeldung am Nessus-Server verwendet.

1. Führen Sie auf den Nessus-Server den Befehl **`nessus-mkcert-client`** aus.

   Linux/UNIX:
   `# /opt/nessus/sbin/nessus-mkcert-client`

   Windows (der Befehl muss als lokaler Administrator ausgeführt werden):
   `C:\> \Programme\Tenable\Nessus\nessus-mkcert-client`

2. Füllen Sie die Felder bei Aufforderung aus. Die Vorgehensweise ist auf Linux-/UNIX- und Windows-Servern identisch.

```
Do you want to register the users in the Nessus server as soon as you create their
       certificates ? [n]: y

--------------------------------------------------------------------------------
                        Creation Nessus SSL client Certificate
--------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
Client certificate life time in days [365]:
Your country (two letter code) [US]:
Your state or province name [NY]: MD
Your location (e.g. town) [New York]: Columbia
Your organization []: Content
Your organizational unit []: Tenable
**********
We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by entering a
       single dot '.'
*********
User #1 name (e.g. Nessus username) []: squirrel
Should this user be administrator? [n]: y
Country (two letter code) [US]:
State or province name [MD]:
Location (e.g. town) [Columbia]:
Organization [Content]:
Organizational unit [Tenable]:
e-mail []:

User rules
----------
nessusd has a rules system which allows you to restrict the hosts that firstuser has
       the right to test. For instance, you may want him to be able to scan his own
       host only.
Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)

User added to Nessus.
```

```
Another client certificate? [n]:
Your client certificates are in C:\Users\admin\AppData\Local\Temp\nessus-0000040e
You will have to copy them by hand
```



Die Clientzertifikate werden in einem systemspezifischen randomisierten Temporärverzeichnis erstellt. Das Temporärverzeichnis ist in der Zeile angegeben, die mit „Your client certificates are in" beginnt.



Installationen von Nessus unter Windows enthalten keine Manpages (lokale Anleitungen). Weitere Informationen zu häufig verwendeten ausführbaren Nessus-Dateien finden Sie im Tenable Support Portal.

3. Im temporären Verzeichnis werden zwei Dateien erstellt, z. B. **cert_squirrel.pem** und **key_squirrel.pem** (wobei „squirrel" der Hostname des in diesem Beispiel verwendeten Systems ist). Diese Dateien müssen kombiniert und in ein Format exportiert werden, das in den Webbrowser importiert werden kann (z. B. **.pfx**). Der folgende **openssl**-Befehl wird hierfür verwendet:

   ```
   # openssl pkcs12 -export -out combined_squirrel.pfx -inkey key_squirrel.pem -in
   cert_squirrel.pem -chain -CAfile /opt/nessus/com/nessus/CA/cacert.pem -passout
   pass:'SecretWord' -name 'Nessus User Certificate for: squirrel'
   ```

   Die resultierende Datei **combined_squirrel.pfx** wird in dem Verzeichnis erstellt, aus dem der Befehl stammte. Die Datei muss dann im Webbrowser in den Speicher mit den persönlichen Zertifikaten importiert werden.

Verbindungen mit Smartcards oder CAC-Karte ermöglichen

Wenn das CAcert für die Smartcard, die CAC oder ein ähnliches Gerät vorhanden ist, müssen die entsprechenden Benutzer in Nessus erstellt werden. Die im Zuge dieses Vorgangs erstellten Benutzer müssen dem CN derjenigen Karte entsprechen, mit der der jeweilige Benutzer sich später anmelden wird.

1. Führen Sie auf dem Nessus-Server den Befehl **nessus-mkcert-client** aus.

   Linux/UNIX:
   ```
   # /opt/nessus/sbin/nessus-mkcert-client
   ```

   Windows (der Befehl muss als lokaler Administrator ausgeführt werden):
   ```
   C:\> \Programme\Tenable\Nessus\nessus-mkcert-client.exe
   ```

2. Füllen Sie die Felder wie erforderlich aus. Die Vorgehensweise ist auf Linux-/UNIX- und Windows-Servern identisch. Der Benutzername muss dem CN entsprechen, der durch das auf der Karte enthaltene Zertifikat angegeben ist.

```
Do you want to register the users in the Nessus server as soon as you create their
      certificates ? [n]: y

  ------------------------------------------------------------------------------
                        Creation Nessus SSL client Certificate
  ------------------------------------------------------------------------------

  This script will now ask you the relevant information to create the SSL
  client certificates for Nessus.
  Client certificate life time in days [365]:
  Your country (two letter code) [US]:
  Your state or province name [NY]: MD
  Your location (e.g. town) [New York]: Columbia
```

```
Your organization []: Content
Your organizational unit []: Tenable
**********
We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by entering a
     single dot '.'
*********
User #1 name (e.g. Nessus username) []: squirrel
Should this user be administrator? [n]: y
Country (two letter code) [US]:
State or province name [MD]:
Location (e.g. town) [Columbia]:
Organization [Content]:
Organizational unit [Tenable]:
e-mail []:

User rules
----------
nessusd has a rules system which allows you to restrict the hosts that firstuser has
the right to test. For instance, you may want him to be able to scan his own host
only.
Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)

User added to Nessus.
Another client certificate? [n]:
Your client certificates are in C:\Users\admin\AppData\Local\Temp\nessus-0000040e
You will have to copy them by hand
```



Die Clientzertifikate werden in einem systemspezifischen randomisierten Temporärverzeichnis erstellt. Das Temporärverzeichnis ist in der Zeile angegeben, die mit „Your client certificates are in“ beginnt. Diese Zertifikate werden für die Kartenauthentifizierung nicht benötigt und können gelöscht werden.

3. Nach der Erstellung kann ein Benutzer mithilfe seiner Karte auf den Nessus-Server zugreifen und sich nach Eingabe seiner PIN oder eines ähnlichen Geheimcodes automatisch authentifizieren.

Verbindung mit Zertifikat oder Kartenunterstützung herstellen

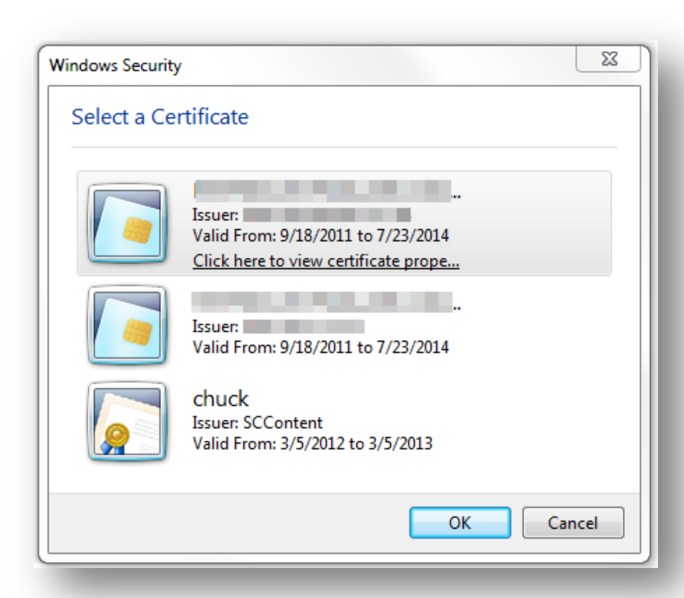


Die nachfolgend beschriebenen Schritte setzen voraus, dass Ihr Browser für die SSL-Zertifikatsauthentifizierung konfiguriert ist. Hierbei ist zu berücksichtigen, dass der Webbrowser der Zertifizierungsstelle ausreichend vertraut. Weitere Informationen zur Konfiguration dieser Funktion entnehmen Sie der Hilfefunktion Ihres Browsers oder anderen Dokumentationen.

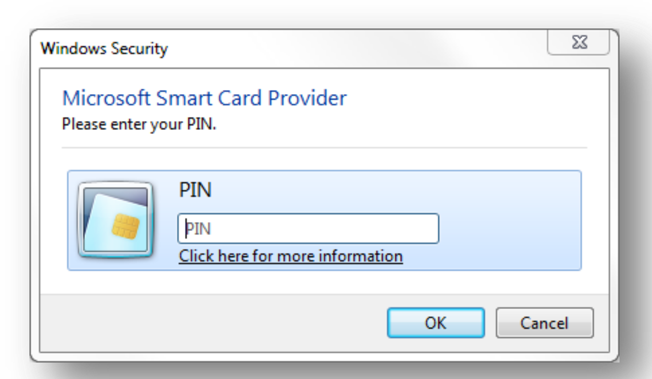
Der Vorgang der zertifikatsgestützten Anmeldung beginnt, wenn ein Benutzer eine Verbindung mit Nessus herstellt.

1. Starten Sie einen Browser und navigieren Sie zum Nessus-Server.

2. Der Browser stellt eine Liste verfügbarer Zertifikatsidentitäten zur Auswahl:



3. Nach der Auswahl eines Zertifikats wird der Benutzer ggf. zur Eingabe der PIN oder eines Kennworts für das Zertifikat aufgefordert. Nach der erfolgreichen Eingabe von PIN oder Kennwort steht das Zertifikat für den weiteren Verlauf der Sitzung zur Verfügung.



4. Wenn der Benutzer zur Nessus-Weboberfläche navigiert, ist das Fenster für die Eingabe von Benutzername und Kennwort kurz sichtbar; die Anmeldung mit dem angegebenen Benutzernamen erfolgt dann automatisch. Nachfolgend kann die Nessus-Benutzeroberfläche normal verwendet werden.



Wenn Sie sich von der Sitzung abmelden, wird der normale Anmeldebildschirm für Nessus angezeigt. Wollen Sie sich mit demselben Zertifikat erneut anmelden, dann wählen Sie die Browserfunktion „Aktualisieren“. Wenn Sie sich mit einem anderen Zertifikat anmelden möchten, müssen Sie Ihre Browsersitzung neu starten.

Nessus ohne Internetzugang

In diesem Abschnitt beschreiben wir die Schritte zur Registrierung des Nessus-Scanners, zur Installation des Aktivierungscodes und zum Empfang der aktuellen Plugins, falls Ihr Nessus-System keinen direkten Zugang zum Internet hat.



Aktivierungscodes, die unter Verwendung des nachfolgend beschriebenen Offlineprozesses abgerufen werden, sind an den Nessus-Scanner gebunden, der bei der Offlineaktualisierung verwendet wird. Sie können das heruntergeladene Plugin-Paket nicht mit einem anderen Nessus-Scanner verwenden.

Führen Sie zunächst die Schritte der mit Nessus bereitgestellten Anleitung aus. Wenn Sie zur Eingabe eines Aktivierungscodes aufgefordert werden, geben Sie „Offline" ein.

Challenge-Code generieren

Sie müssen Ihren Aktivierungscode entweder über Ihr Tenable Support Portal-Konto abrufen (Nessus) oder Ihrer Registrierungs-E-Mail entnehmen (Nessus Home).

Beachten Sie, dass Sie nur einen Aktivierungscode je Scanner einsetzen können, sofern die Scanner nicht über SecurityCenter verwaltet werden.

Sobald Sie über den Aktivierungscode verfügen, führen Sie den folgenden Befehl auf dem System aus, auf dem Nessus ausgeführt wird:

Windows:
```
C:\Programme\Tenable\Nessus>nessus-fetch.exe --challenge
```

Linux:
```
# /opt/nessus/bin/nessus-fetch --challenge
```

FreeBSD:
```
# /usr/local/nessus/bin/nessus-fetch --challenge
```

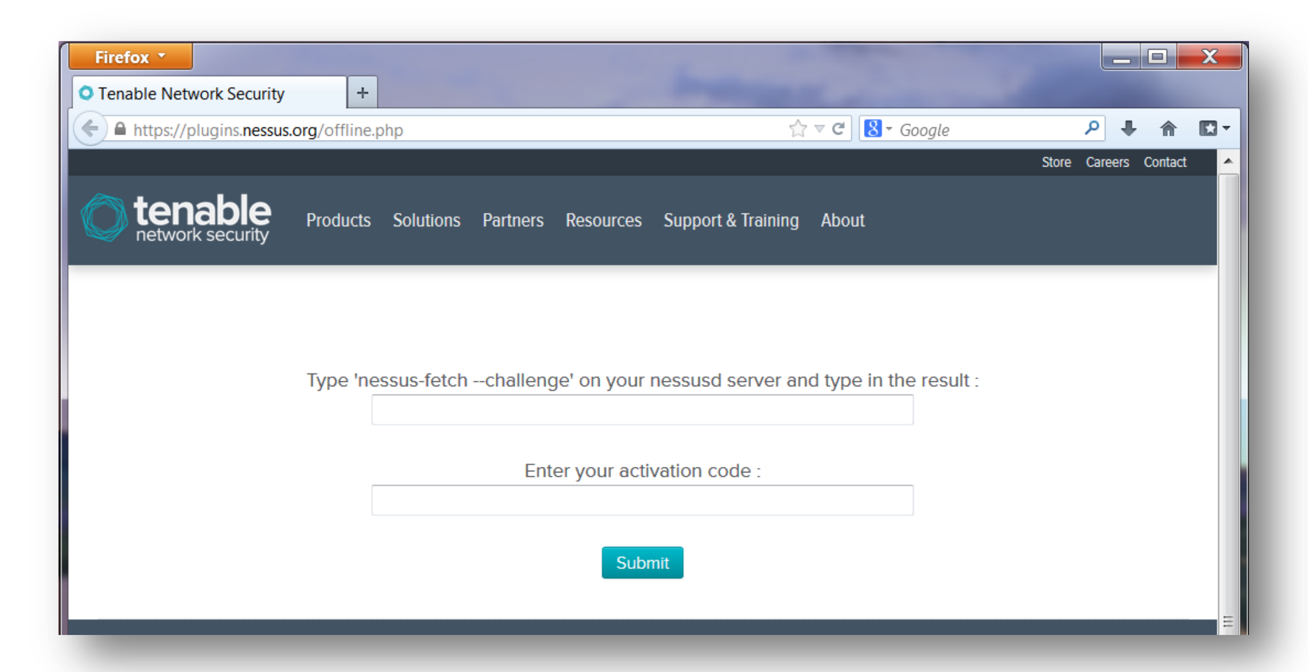
Mac OS X:
```
# /Library/Nessus/run/bin/nessus-fetch --challenge
```

Hiermit wird eine Zeichenfolge erstellt, die als „Challenge" bezeichnet wird und wie folgt aussieht:

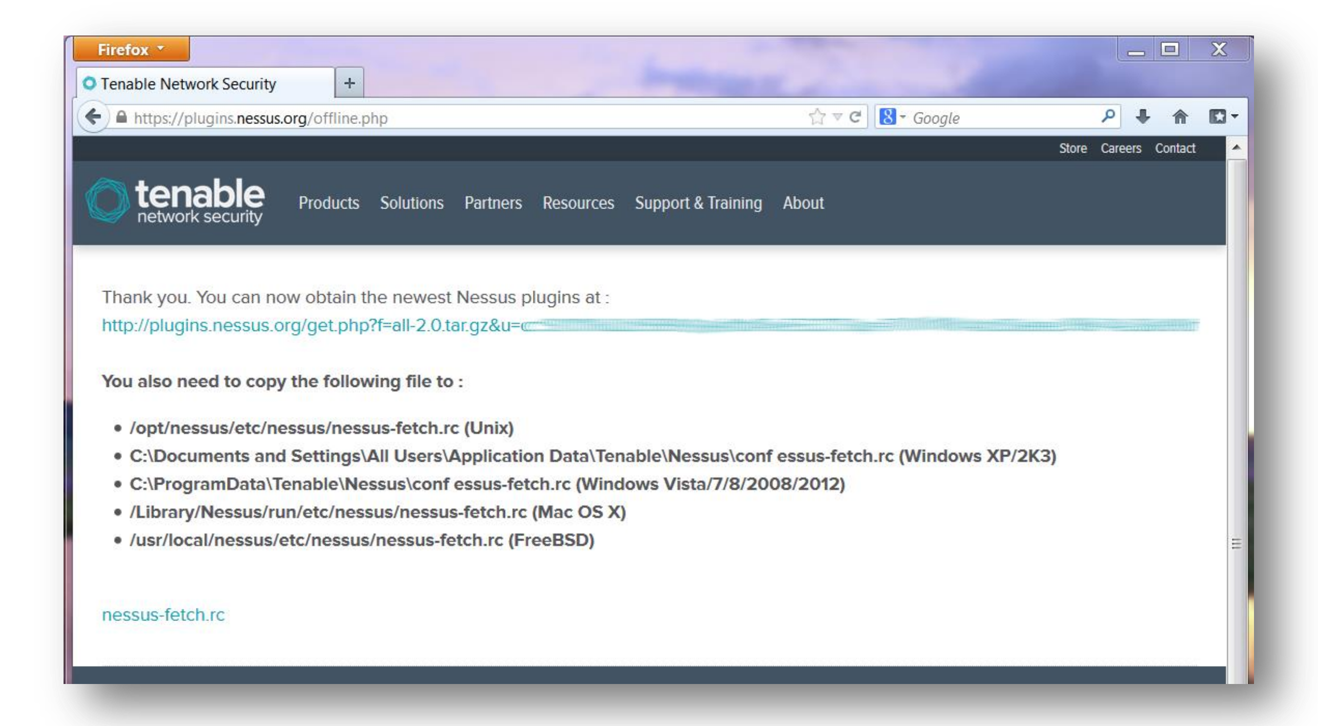
```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Aktuelle Plugins beziehen und installieren

Nun rufen Sie die Seite https://plugins.nessus.org/offline.php auf und kopieren die Challenge sowie den zuvor erhaltenen Aktivierungscode über die Zwischenablage in die entsprechenden Textfelder:



Daraufhin wird eine URL ähnlich der in der folgenden Bildschirmabbildung gezeigten generiert:



Auf diesem Bildschirm haben Sie die Möglichkeit, die aktuellen Nessus-Plugins als gepackte Datei (**`all-2.0.tar.gz`**) herunterzuladen. Außerdem finden Sie am unteren Bildschirmrand einen Link auf die Datei **`nessus-fetch.rc`**.



Diese URL müssen Sie speichern, denn Sie benötigen sie immer dann, wenn Sie Ihre Plugins wie nachfolgend beschrieben aktualisieren möchten.



Ein Registrierungscode, der für Offlineupdates verwendet wird, kann im Nessus Server Manager nicht für denselben Nessus-Scannerserver verwendet werden.

Führen Sie folgenden Befehl zur Offlineregistrierung von Nessus aus, und installieren Sie die Datei **`nessus-fetch.rc`** im Nessus Verzeichnis auf dem Host:

Windows XP/2003:
```
C:\Programme\Tenable\Nessus>nessus-fetch.exe --register-offline "C:\Dokumente und Einstellungen\All Users\Application Data\Tenable\Nessus\conf\nessus-fetch.rc"
```

Windows Vista/7/8/2008/2012:
```
C:\Programme\Tenable\Nessus>nessus-fetch.exe --register-offline "C:\ProgramData\Tenable\Nessus\conf\nessus-fetch.rc"
```

Hinweis: Der Speicherort der Konfigurationsdateien wurde beim Update von Nessus 5.0 auf Version 5.2 geändert.

Linux:
```
# /opt/nessus/bin/nessus-fetch --register-offline /opt/nessus/etc/nessus/nessus-fetch.rc
```

FreeBSD:
```
# /usr/local/nessus/bin/nessus-fetch --register-offline /usr/local/nessus/etc/nessus/nessus-fetch.rc
```

Mac OS X:
```
# /Library/Nessus/run/bin/nessus-fetch --register-offline /Library/Nessus/run/etc/nessus/nessus-fetch.rc
```

Beachten Sie, dass Nessus nach der Registrierung standardmäßig alle 24 Stunden versuchen wird, die Plugins zu aktualisieren. Wenn Sie diesen Versuch, online zu gehen, unterbinden möchten, setzen Sie die Option **`auto_update`** unter „**Configuration**“ > „**Advanced**“ („Konfiguration“ > „Erweitert“) auf „**`no`**“ („Nein“).



Führen Sie diesen Schritt jedes Mal aus, wenn Sie ein Offlineupdate Ihrer Plugins ausführen.

Verschieben Sie nach dem Herunterladen die Datei **`all-2.0.tar.gz`** in das Nessus-Verzeichnis. Dann starten Sie die Verarbeitung des Plugin-Archivs in Nessus:

Windows:
```
C:\Programme\Tenable\Nessus>nessus-update-plugins.exe all-2.0.tar.gz
```

UNIX (passen Sie den Pfad an Ihre Installation an):
```
# /opt/nessus/sbin/nessus-update-plugins all-2.0.tar.gz
```

Nach der Verarbeitung muss Nessus neu gestartet werden, um die Änderungen zu übernehmen. Angaben zum Neustart finden Sie in den Abschnitten „Nessus-Dienst über die Windows-Befehlszeile steuern“ bzw. „Den Nessus-Daemon starten/beenden“ (UNIX).

Nach der Installation der Plugins können Sie die Datei **`all-2.0.tar.gz`** eigentlich löschen; Tenable empfiehlt jedoch, die jeweils aktuellste Version der heruntergeladenen Plugin-Datei für den Fall aufzubewahren, dass sie noch einmal benötigt wird.

Die aktuellen Plugins stehen Ihnen jetzt zur Verfügung. Jedes Mal, wenn Sie eine Aktualisierung Ihrer Plugins ohne Internetverbindung ausführen möchten, müssen Sie die angegebene URL aufrufen, die **`tar`**/**`gz`**-Datei laden, sie auf das System kopieren, auf dem Nessus ausgeführt wird, und den obigen Vorgang wiederholen.

Nessus über die Befehlszeile verwenden und verwalten

Die wichtigsten Nessus-Verzeichnisse

In der folgenden Tabelle sind die Installationsposition und wichtige Verzeichnisse aufgelistet, die von Nessus unter *NIX/Linux verwendet werden:

Nessus-Stammverzeichnis	Nessus-Unterverzeichnisse	Zweck
UNIX-Distributionen		
Red Hat, SuSE, Debian, Ubuntu: `/opt/nessus`	`./etc/nessus/`	Konfigurationsdateien
	`./var/nessus/users/<username>/kbs/`	Auf Festplatte gespeicherte User-Knowledge-Base
FreeBSD: `/usr/local/nessus`	`./lib/nessus/plugins/`	Nessus-Plugins
Mac OS X: `/Library/Nessus/run`	`./var/nessus/logs/`	Nessus-Logdateien

In der folgenden Tabelle sind die Installationsposition und wichtige Verzeichnisse aufgelistet, die von Nessus unter Windows verwendet werden:

Nessus-Stammverzeichnis	Nessus-Unterverzeichnisse	Zweck
Windows		
`\Programme\Tenable\Nessus`	`\conf`	Konfigurationsdateien
	`\data`	Stylesheetvorlagen
	`\nessus\plugins`	Nessus-Plugins
	`\nessus\users\<Benutzername>\kbs`	Auf Festplatte gespeicherte User-Knowledge-Base
	`\nessus\logs`	Nessus-Logdateien

Nessus-Benutzer mit Kontenbeschränkungen erstellen und verwalten

Ein einzelner Nessus-Scanner kann einen komplexen Aufbau mit mehreren Benutzern unterstützen. Denkbar ist beispielsweise, dass in einem Unternehmen mehrere Mitarbeiter Zugriff auf denselben Nessus-Scanner haben, mit

diesem aber jeweils unterschiedliche IP-Bereiche gescannt werden sollen. Für solche Fälle lassen sich die zu scannenden IP-Bereiche einschränken.

Das folgende Beispiel veranschaulicht die Erstellung eines zweiten Nessus-Benutzers mit Kennwortauthentifizierung und Benutzerregeln, mit denen der Benutzer lediglich das Klasse-B-Netzwerk 172.20.0.0/16 scannen kann. Weitere Beispiele und die Syntax der Benutzerregeln finden Sie in den Manpages zu **nessus-adduser**.

```
# /opt/nessus/sbin/nessus-adduser
Login : tater-nessus
Login password :
Login password (again) :
Soll dieser Benutzer ein Nessus ‚admin' Benutzer sein ? (kann Plugins hochladen,
       usw...) (j/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that tater-nessus has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
accept 172.20.0.0/16
deny 0.0.0.0/0



Login : tater-nessus
Password: ***********
This user will have 'admin' privileges within the Nessus server
Rules
accept 172.20.0.0/16
deny 0.0.0.0/0
Stimmt das so ? (y/n) [y] y
User added
```



Zur Anzeige der Manpage für nessus-adduser(8) müssen Sie unter bestimmten Betriebssystemen die folgenden Befehle ausführen:

```
# export MANPATH=/opt/nessus/man
# man nessus-adduser
```

Befehlszeilenoptionen für nessusd

Zusätzlich zur einfachen Ausführung des **nessusd**-Servers gibt es eine Reihe von Befehlszeilenoptionen, die nach Bedarf verwendet werden können. Die folgende Tabelle enthält Informationen zu diesen optionalen Befehlen.

Option	Beschreibung
-c <Konfigurationsdatei>	Beim Start des **nessusd**-Servers kann mithilfe dieser Option die zu verwendende serverseitige **nessusd**-Konfigurationsdatei angegeben werden. Dies ermöglicht die Verwendung einer alternativen Konfigurationsdatei anstelle der Standarddatei **/opt/nessus/etc/nessus/nessusd.db** (bzw.

	`/usr/local/nessus/etc/nessus/nessusd.db` für FreeBSD).
-a <Adresse>	Beim Start des **nessusd**-Servers kann mithilfe dieser Option festgelegt werden, dass der Server nur auf Verbindungen mit der Adresse **<Adresse>** horcht. Hierbei handelt es sich um eine IP-Adresse (d. h. nicht um einen Computernamen). Diese Option ist nützlich, wenn Sie **nessusd** auf einem Gateway ausführen und vermeiden möchten, dass von außen eine Verbindung mit Ihrem **nessusd** hergestellt werden kann.
-S <ip[,ip2,...]>	Erzwingen Sie beim Start des **nessusd**-Servers mit diesem Befehl die Festlegung der IP-Absenderadresse von Verbindungen, die von Nessus während des Scanvorgangs hergestellt werden, auf **<ip>**. Diese Option ist nur dann von Nutzen, wenn Sie einen Multihomed-Computer mit mehreren öffentlichen IP-Adressen einsetzen, die statt der Standardadresse verwendet werden sollen. Damit eine solche Konfiguration funktioniert, muss der Host, auf dem **nessusd** ausgeführt wird, über mehrere Netzwerkkarten mit entsprechend festgelegten IP-Adressen verfügen.
-p <Portnummer>	Beim Start des **nessusd**-Servers kann dieser mithilfe dieser Option angewiesen werden, auf Clientverbindungen über den Port **<Portnummer>** statt über den Standardport 1241 zu horchen.
-D	Beim Start des **nessusd**-Servers wird mithilfe dieser Option festgelegt, dass der Server im Hintergrund ausgeführt wird (Daemon-Modus).
-v	Zeigt die Versionsnummer an und wird dann beendet.
-l	Zeigt die Plugin-Feedlizenz an und wird dann beendet.
-h	Zeigt eine Befehlszusammenfassung an und wird dann beendet.
--ipv4-only	Es wird nur auf dem IPv4-Socket gehorcht.
--ipv6-only	Es wird nur auf dem IPv6-Socket gehorcht.
-q	Betrieb im „stillen“ Modus (alle Meldungen an **stdout** werden unterdrückt).
-R	Erzwingt eine Neuverarbeitung der Plugins.
-t	Überprüft die Zeitstempel aller Plugins beim Start, damit nur frisch aktualisierte Plugins kompiliert werden.
-K	Hiermit wird ein Masterkennwort für den Scanner festgelegt.

Wenn ein Masterkennwort festgelegt wird, verschlüsselt Nessus alle Richtlinien und die darin enthaltenen Anmeldedaten mit dem durch den Benutzer angegebenen Schlüssel (dieser ist erheblich sicherer als der Standardschlüssel). Wird ein Kennwort festgelegt, dann werden Sie beim Start über die Weboberfläche aufgefordert, es einzugeben.



ACHTUNG: Wenn das Masterkennwort festgelegt wurde und dann verloren geht, kann es weder durch Ihren Administrator noch durch den Tenable-Support wiederhergestellt werden.

Nachfolgend gezeigt ist ein Einsatzbeispiel:

Linux:

```
# /opt/nessus/sbin/nessus-service [-vhD] [-c <Konfigurationsdatei>] [-p <Portnummer>] [-a <address>] [-S <ip[,ip,...]>]
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-service [-vhD] [-c <Konfigurationsdatei>] [-p <Portnummer>] [-a <address>] [-S <ip[,ip,...]>]
```

Nessus-Dienst über die Windows-Befehlszeile steuern

Nessus kann auch über die Befehlszeile gestartet oder beendet werden. Beachten Sie, dass das Befehlszeilenfenster mit Administratorrechten aufgerufen werden muss:

```
C:\Windows\system32>net stop "Tenable Nessus"
The Tenable Nessus service is stopping.
The Tenable Nessus service was stopped successfully.


C:\Windows\system32>net start "Tenable Nessus"
The Tenable Nessus service is starting.
The Tenable Nessus service was started successfully.


C:\Windows\system32>
```

Mit SecurityCenter arbeiten

SecurityCenter im Überblick

Tenable SecurityCenter ist eine webbasierte Verwaltungskonsole, die den Prozess der Sicherheitslückenerkennung und -verwaltung, Ereignis- und Logdateiverwaltung, Compliance-Überwachung und eine Berichtserstellungsfunktion für alle genannten Vorgänge auf einer einheitlichen Oberfläche zusammenfasst. SecurityCenter ermöglicht eine effiziente Kommunikation sicherheitsrelevanter Ereignisse an IT-, Verwaltungs- und Auditteams.

SecurityCenter unterstützt die koordinierte Nutzung mehrerer Nessus-Scanner, um Netzwerke praktisch beliebiger Größe regelmäßig zu scannen. Mithilfe der Nessus-API (einer angepassten Implementierung des XML-RPC-Protokolls) kommuniziert SecurityCenter mit den zugeordneten Nessus-Scannern, um Anweisungen an diese zu übermitteln und Resultate abzurufen.

SecurityCenter ermöglicht mehreren Benutzern und Administratoren unterschiedlicher Sicherheitsstufen die Freigabe von Informationen zu Sicherheitslücken, eine Priorisierung der Sicherheitslücken, das Auflisten von Netzwerk-Assets, die kritische Sicherheitsprobleme aufweisen, das Empfehlen von durch Systemadministratoren zur Behebung dieser Sicherheitsprobleme durchzuführenden Maßnahmen und schließlich die Überprüfung, ob die Sicherheitslücke geschlossen wurde. SecurityCenter ruft außerdem über die Log Correlation Engine (LCE) Daten von zahlreichen führenden Intrusion-Detection-Systemen wie Snort oder ISS ab.

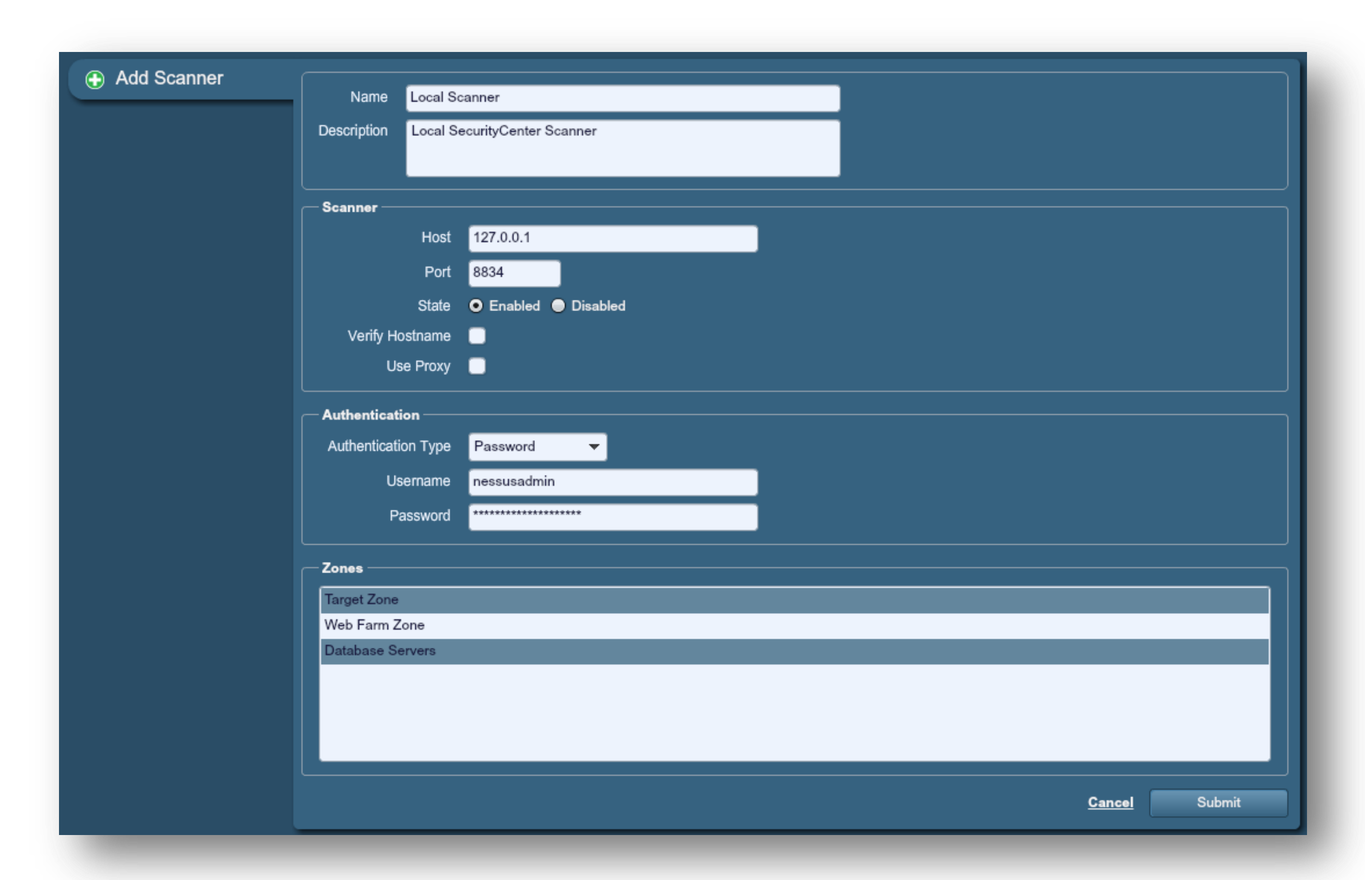
Außerdem kann SecurityCenter auch passive Sicherheitslückeninformationen vom Tenable Passive Vulnerability Scanner (PVS) abrufen, damit Endbenutzer neue Hosts, Anwendungen, Sicherheitslücken und unbefugtes Eindringen auch ohne aktives Scannen mit Nessus ermitteln können.

SecurityCenter für die Kooperation mit Nessus konfigurieren

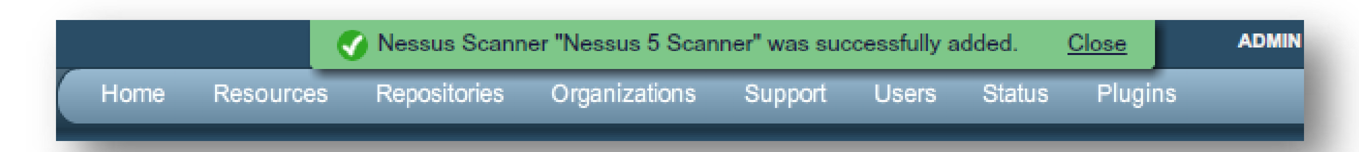
Mithilfe der SecurityCenter-Verwaltungsoberfläche können Zugriff und Steuerung beliebiger Nessus-Scanner mit der Versionsnummer 4.2.x oder höher konfiguriert werden. Klicken Sie auf die Registerkarte „**Resources**“ („Ressourcen“) und dann auf „**Nessus Scanners**“. Klicken Sie auf „**Add**“ („Hinzufügen“), um das Dialogfeld „**Add Scanner**“ („Scanner hinzufügen“) zu öffnen. Angegeben werden müssen die IP-Adresse oder der Hostname des Nessus-Scanners, der Nessus-Port (Standard: 8834), der bei der Konfiguration von Nessus erstellte Authentifizierungstyp, der Anmeldename des Administrators und das zugehörige Kennwort oder die erforderlichen Zertifikatsinformationen sowie ein Name. Die

Kennwortfelder sind nicht verfügbar, wenn die Authentifizierung via SSL-Zertifikat (Option „SSL Certificate“) ausgewählt wird. Die Funktion zur Überprüfung des Hostnamens ermöglicht die Verifizierung des CN (Common Name) im SSL-Zertifikat, das vom Nessus-Server übermittelt wurde. Der Status des Nessus-Scanners kann bei Bedarf auf „Enabled“ („Aktiviert“) oder „Disabled“ („Deaktiviert“) gesetzt werden. Zudem können die Verwendung des Proxys und eine Reihe von Scanzones, denen der Nessus-Scanner zugewiesen ist, ausgewählt werden.

Nachfolgend gezeigt ist eine Bildschirmabbildung der Seite „**Add Scanner**“ aus SecurityCenter 4.7:



Nach dem erfolgreichen Hinzufügen des Scanners wird das folgende Banner angezeigt:



Weitere Informationen zur Integration von Nessus und SecurityCenter finden Sie im „SecurityCenter-Administrationshandbuch“ im Tenable Support Portal.

Hostbasierte Firewalls

Wenn Ihr Nessus-Server mit einer Personal Firewall wie beispielsweise Zone Alarm, BlackICE, der Windows XP Firewall oder einer anderen Firewallsoftware konfiguriert ist, müssen Verbindungsanfragen von der IP-Adresse von SecurityCenter zugelassen werden.

Standardmäßig ist Port 8834 zur Kommunikation mit SecurityCenter vorgesehen. Auf Systemen unter Microsoft XP Service Pack 2 und höher erhält der Benutzer nach Klick auf das Symbol „**Sicherheitscenter**“ in der „**Systemsteuerung**“ die Möglichkeit, die Einstellungen der Windows-Firewall zu verwalten. Um Port 8834 zu öffnen, wählen Sie die Registerkarte „**Ausnahmen**“ aus und fügen Port 8834 zur Liste hinzu.

Problembehandlung bei Nessus für Windows

Installations- und Upgradeprobleme

Problem: Laut der Logdatei „nessusd.messages“ wurde „nessusd“ gestartet, was offensichtlich aber nicht zutrifft.

Lösung: Die Meldung „nessusd <Version> started“ („nessusd <Version> wurde gestartet“) gibt nur an, dass das Programm `nessusd` ausgeführt wurde. Die Meldung „nessusd is ready“ hingegen besagt, dass der Nessus-Server ausgeführt wird und Verbindungen annehmen kann.

Problem: Ich erhalte bei dem Versuch, Nessus Windows zu installieren, folgende Fehlermeldung:

„1607: Unable to install InstallShield Scripting Runtime“ („Die InstallShield Scripting-Laufzeit kann nicht installiert werden“)

Lösung: Dieser Fehlercode wird erzeugt, wenn der WMI-Dienst (Windows Management Instrumentation) deaktiviert wurde. Vergewissern Sie sich, dass der Dienst ausgeführt wird.

Wenn der WMI-Dienst ausgeführt wird, kommt als Ursache ein Konflikt zwischen den Einstellungen des Microsoft Windows-Betriebssystems und dem InstallShield-Produkt in Frage, mit dem Nessus Windows installiert und entfernt wird. Knowledge-Base-Artikel, die mögliche Ursachen und Lösungen zu diesem Problem beschreiben, wurden sowohl von Microsoft als auch von InstallShield veröffentlicht.

- Microsoft Knowledge-Base-Artikel 910816:
  http://support.microsoft.com/?scid=kb;en-us;910816
- InstallShield Knowledge-Base-Artikel Q108340:
  http://consumer.installshield.com/kb.asp?id=Q108340

Probleme beim Scannen

Problem: Ich kann über meine PPP- oder PPTP-Verbindung keine Scans ausführen.

Lösung: Gegenwärtig wird diese Vorgehensweise nicht unterstützt. Zukünftige Versionen von Nessus Windows werden jedoch eine solche Funktionalität enthalten.

Problem: Ein Virenscan meines Systems meldet eine große Zahl Viren oder Malware in Nessus Windows.

Lösung: Bestimmte Antivirenprogramme melden einige Nessus-Plugins als Viren. Schließen Sie das Plugin-Verzeichnis vom Virenscan aus. Das Verzeichnis enthält keine ausführbaren Dateien. Weitere Informationen zum Einsatz von Nessus in Verbindung mit Software zur Malwarebekämpfung finden Sie im Dokument „Nessus 5 und Virenschutz“.

Problem: Ich scanne ein ungewöhnliches Gerät (z. B. einen RAID-Controller), und der Scan wird abgebrochen, weil es von Nessus als Drucker erkannt wird.

Lösung: Deaktivieren Sie die Option „Safe Checks“ in der Scanrichtlinie, bevor Sie das Gerät scannen. Der Scan eines Druckers führt gewöhnlich dazu, dass der Drucker neu gestartet werden muss. Aus diesem Grund werden, wenn „Safe Checks“ festgelegt ist, als Drucker erkannte Geräte nicht gescannt.

Problem: Bei SYN-Scans wird offenbar nicht darauf gewartet, dass die Portverbindung in Nessus Windows hergestellt wird.

Lösung: Dies ist insofern korrekt, als bei einem SYN-Scan keine vollständige TCP-Verbindung aufgebaut wird. Allerdings hat dies keine Auswirkungen auf die Scanergebnisse.

Problem: Welche Faktoren wirken sich bei der Durchführung eines Scans auf die Leistung aus, wenn Nessus Windows auf einem Windows XP-System ausgeführt wird?

Lösung: Microsoft hat an Windows XP SP 2 und SP 3 (und zwar sowohl bei der Home- als auch bei der Professional-Version) Änderungen vorgenommen, die die Leistungsfähigkeit von Nessus Windows beeinträchtigen und Fehlalarme auslösen können. Der TCP/IP-Stapel beschränkt nun die Anzahl gleichzeitiger unvollständiger ausgehender TCP-Verbindungsversuche. Wenn dieses Limit erreicht wurde, werden nachfolgende Verbindungsversuche in eine Warteschlange eingereiht und mit festgelegter Geschwindigkeit (zehn Verbindungsversuche pro Sekunde) aufgelöst. Wenn die Warteschlange zu lang wird, werden möglicherweise Verbindungsanfragen verworfen. Die folgende Microsoft TechNet-Seite enthält weitere Informationen:

http://technet.microsoft.com/en-us/library/bb457156.aspx

Dies hat zur Folge, dass ein Nessus-Scan unter Windows XP unter Umständen Fehlalarme produziert, denn Windows XP gestattet lediglich zehn neue Verbindungen pro Sekunde, die nicht abgeschlossen sind (d. h. den SYN-Zustand aufweisen). Zur Genauigkeitsverbesserung wird empfohlen, die Drosselungseinstellungen für Portscans bei Nessus auf einem Windows XP-System auf die folgenden Werte zu verringern (Sie finden die Parameter in der Scankonfiguration der jeweiligen Scanrichtlinie):

Max number of hosts (maximale Anzahl Hosts): 10
Max number of security checks (maximale Anzahl Sicherheitstests): 4

Um die Leistungsfähigkeit und die Zuverlässigkeit von Scans zu steigern, wird dringend empfohlen, Nessus Windows unter einem Serverprodukt der Microsoft Windows-Familie (z. B. Windows Server 2003 oder Windows Server 2008) zu installieren.



Bitte beachten Sie, dass die Unterstützung für Windows XP ab Nessus 5.3 vollständig entfallen wird.

Weitere Informationen

Tenable hat eine Reihe von Dokumenten erstellt, in denen die Bereitstellung, die Konfiguration, der Betrieb und die Testmethoden von Nessus ausführlich beschrieben werden. Es sind diese:

- **Nessus 5.2 User Guide** („Nessus 5.2-Benutzerhandbuch"; beschreibt den Einsatz des Nessus Nessus-Sicherheitslückenscanners einschließlich Konfiguration und Berichterstellung)
- **Nessus Credential Checks for Unix and Windows** („Authentifizierte Nessus-Tests für UNIX und Windows"; enthält Informationen zur Durchführung authentifizierter Netzwerkscans mit dem Nessus-Sicherheitslückenscanner)
- **Nessus Compliance Checks** („Nessus-Compliancetests"; allgemeiner Leitfaden zum Verständnis und zur Durchführung von Compliancetests mithilfe von Nessus und SecurityCenter)

- **Nessus Compliance Checks Reference** („Nessus-Referenzhandbuch für Compliancetests"; umfassender Leitfaden zur Syntax von Nessus-Compliancetests)

- **Nessus v2 File Format** („Nessus V2-Dateiformat"; beschreibt die Struktur des `.nessus`-Dateiformats, das mit Nessus 3.2 und NessusClient 3.2 eingeführt wurde)

- **Nessus 5.0 REST Protocol Specification** („Nessus 5.0 REST-Protokollspezifikation"; beschreibt das REST-Protokoll und die Schnittstelle in Nessus)

- **Nessus 5 and Antivirus** („Nessus 5 und Virenschutz"; beschreibt die Funktion verschiedener gängiger Sicherheitssoftwarepakete in Nessus und enthält Tipps und Lösungsvorschläge für eine verbesserte Funktionsweise der Software ohne Einschränkung der Sicherheit oder Verhinderung Ihrer Sicherheitslückenscans)

- **Nessus 5 and Mobile Device Scanning** („Nessus 5 und Scans von Mobilgeräten"; beschreibt die Integration von Nessus in Microsoft Active Directory und Verwaltungsserver für Mobilgeräte zur Bestimmung von im Netzwerk eingesetzten Mobilgeräten)

- **Nessus 5.0 and Scanning Virtual Machines** („Nessus 5.0 und Scans virtueller Maschinen"; beschreibt den Einsatz des Sicherheitslückenscanners von Tenable Network Security Nessus für Audits der Konfiguration virtueller Plattformen sowie der darauf ausgeführten Software)

- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE** („Strategische Malwareüberwachung mit Nessus, PVS und LCE"; beschreibt, wie mithilfe der Tenable USM-Plattform zahlreiche bösartige Softwareprogramme erkannt werden können und das Ausmaß der Malware-Infizierung bestimmt werden kann)

- **Patch Management Integration** („Integration des Patchmanagements"; beschreibt, wie Nessus und SecurityCenter mithilfe von Berechtigungen auf die IBM TEM-, Microsoft WSUS- und SCCM-, VMware Go- und Red Hat Network Satellite-Patchmanagementsysteme Patch-Audits auf Systemen ausführen, für die dem Nessus-Scanner möglicherweise keine Berechtigungen zur Verfügung stehen)

- **Real-Time Compliance Monitoring** („Compliance-Überwachung in Echtzeit"; erläutert, wie die Lösungen von Tenable Sie bei der Erfüllung zahlreicher gesetzlicher Vorschriften und Finanzstandards unterstützen)

- **Tenable Products Plugin Families** („Tenable Produkt-Plugin-Familien"; stellt eine Beschreibung und Zusammenfassung der Plugin-Serien für Nessus, Log Correlation Engine und den Passive Vulnerability Scanner bereit)

- **SecurityCenter Administration Guide** („SecurityCenter-Administratorhandbuch")

Weitere Onlineressourcen sind nachfolgend aufgeführt:

- Nessus-Diskussionsforum: https://discussions.nessus.org/

- Tenable-Blog: http://www.tenable.com/blog

- Tenable-Podcast: http://www.tenable.com/podcast

- Beispielvideos zum Gebrauch: http://www.youtube.com/user/tenablesecurity

- Tenable-Twitterfeed: http://twitter.com/tenablesecurity

Setzen Sie sich mit uns in Verbindung – via E-Mail (support@tenable.com, sales@tenable.com) oder über unsere Website unter http://www.tenable.com/.

Wissenswertes zu Tenable Network Security

Wenn es um die frühzeitige Erkennung neu entwickelter Sicherheitslücken, Bedrohungen und Compliance-relevanter Risiken geht, verlassen sich mehr als 20.000 Organisationen auf Tenable Network Security. Hierzu gehören neben dem gesamten US-Verteidigungsministerium eine Reihe von Großunternehmen und Regierungsbehörden weltweit. Die Nessus- und SecurityCenter-Lösungen sind nach wie vor branchenführend beim Ermitteln von Sicherheitslücken, beim Verhindern von Angriffen und bei der Erfüllung einer Vielzahl gesetzlicher Vorschriften. Weitere Informationen finden Sie unter www.tenable.com.

GLOBALE UNTERNEHMENSZENTRALE

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046, USA
+1.410.872.0555
www.tenable.com

